Declaratia practicilor aplicabile serviciilor de incredere furnizate de Alfatrust Certification S.A.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

Cuprins

1. Introducere7
   - 1.1. Rolul DPSI7
   - 1.2. Servicii de incredere7
   - 1.3. Privire de ansamblu asupra infrastructurii de certificare8
   - 1.4. Sfera de aplicabilitate10
     - 1.4.1. Sfera de aplicabilitate a DPSI10
     - 1.4.2. Sfera de aplicabilitate a certificatelor emise de AlfaTrust Certification11
     - 1.4.3. Autoritati de certificare (AC)13
     - 1.4.4. Autoritati de inregistrare (AI)14
     - 1.4.5. Autoritatea de Marcare Temporala (TSA)14
     - 1.4.6. Autoritatea de Validare (AV)14
     - 1.4.7. Utilizatorii finali si entitatile partenere15
   - 1.5. Detalii de contact15
2. Dispozitii generale16
   - 2.1. Obligatii16
     - 2.1.1. Obligatiile Autoritatii de Certificare (AC)16
     - 2.1.2. Obligatiile Autoritatii de Inregistrare (AI)17
     - 2.1.3. Obligatiile Autoritatii de Marcare Temporala (TSA)18
     - 2.1.4. Obligatiile Autoritatii de Validare (AV)19
     - 2.1.5. Obligatiile utilizatorului final19
     - 2.1.6. Obligatiile entitatilor partenere21
   - 2.2. Responsabilitati23
     - 2.2.1. Responsabilitatea Furnizorului de Servicii de Certificare (FSC)23
     - 2.2.2. Responsabilitatea utilizatorului23
     - 2.2.3. Responsabilitatea partilor contractante24
   - 2.3. Responsabilitati financiare24
   - 2.4. Legea aplicabila si solutionarea litigiilor24
   - 2.5. Pretul serviciilor prestate25
   - 2.6. Publicarea si inregistrarea informatiilor25
     - 2.6.1. Publicarea informatiilor de catre AlfaTrust Certification S.A.25

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.6.2. Frecventa publicarii26
2.6.3. Controlul accesului la informatii26
2.7. Evaluarea conformitatii27
2.8. Confidentialitate27
2.9. Drepturi de proprietate intelectuala29
3. Identificare si autentificare30
3.1. Inregistrarea initiala30
3.1.1. Tipuri de nume30
3.1.2. Necesitatea ca numele sa aiba sens31
3.1.3. Unicitatea numelor32
3.1.4. Procedura aplicabila in litigiile referitoare la dreptul la nume32
3.1.5. Autentificarea identitatii persoanelor juridice33
3.1.6. Autentificarea identitatii persoanelor fizice34
3.1.7. Autentificarea dispozitivelor34
3.2. Autentificarea identitatii la reinnoirea sau modificarea certificatului35
3.2.1. Reinnoirea unui certificat35
3.2.2. Modificarea unui certificat35
3.3. Autentificarea identitatii la revocarea unui certificat36
4. Cerinte operationale36
4.1. Trimiterea cererii36
4.1.1. Cererea de inregistrare37
4.1.2. Cererea de reinnoire sau modificare certificat37
4.1.3. Cererea de revocare a unui certificat37
4.2. Tratarea cererilor de certificare38
4.2.1. La Autoritatea de Inregistrare (AI)38
4.2.2. La Autoritatea de Certificare (AC)38
4.2.3. Emiterea certificatelor39
4.2.4. Respingerea cererii de certificat39
4.2.5. Acceptarea certificatelor40
4.3. Revocarea certificatelor40
4.3.1. Circumstantele revocarii certificatului41
4.3.2. Cine poate solicita revocarea42
4.3.3. Procedura de revocare42

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

4.3.4. Frecventa de emitere a CRL-urilor43
4.3.5. Verificarea listei de certificate revocate (CRL)44
4.3.6. Verificarea on-line a starii certificatelor (OCSP)44
4.3.7. Revocarea certificatului Autoritatii de Certificare (AC)45
4.4. Schimbarea cheii unei Autoritati de Certificare (AC)45
4.5. Incetarea activitatii unui Furnizor de Servicii de Certificare (FSC) sau transferarea serviciilor45
4.5.1. Transferul responsabilitatii46
4.5.2. Emiterea certificatelor de catre succesor46
5. Masurile de securitate InfoSEC46
5.1. Controale ComSEC47
5.1.1. Controale de securitate criptografica (cryptosecurity)47
5.1.1.1. Generarea si folosirea perechii de chei47
5.1.1.1.1. Generarea perechilor de chei47
5.1.1.1.2. Distribuirea cheii private50
5.1.1.1.3. Distribuirea cheii publice catre Autoritatea de Certificare (AC)50
5.1.1.1.4. Distribuirea cheii publice a Autoritatii de Certificare (AC)51
5.1.1.1.5. Dimensiunea cheilor51
5.1.1.1.6. Parametrii de generare a cheilor publice si verificarea calitatii parametrilor51
5.1.1.1.7. Generarea cheilor hardware si/sau software51
5.1.1.1.8. Folosirea cheilor52
5.1.1.2. Protectia cheii private52
5.1.1.2.1. Standarde pentru modulele criptografice52
5.1.1.2.2. Controlul dual al accesului cheii private53
5.1.1.2.2.1. Acceptarea pastrarii secretului de catre detinatori53
5.1.1.2.2.2. Protectia secretului partajat54
5.1.1.2.2.3. Disponibilitatea si stergerea (transferul) secretului partajat54
5.1.1.2.2.4. Responsabilitatile detinatorului de secret partajat54
5.1.1.2.3. Back-up-ul cheilor private54
5.1.1.2.4. Arhivarea cheii private55
5.1.1.2.5. Introducerea cheii private in modulul criptografic55
5.1.1.2.6. Metoda de activare a cheii private55
5.1.1.2.7. Metoda de dezactivare a cheii private56
5.1.1.2.8. Metoda de distrugere a cheii private56

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.1.1.3. Alte aspecte cu privire la managementul perechilor de chei56
5.1.1.3.1. Arhivarea cheilor publice57
5.1.1.3.2. Perioadele de folosire a cheilor private si publice57
5.1.1.4. Datele de activare57
5.1.1.4.1. Generarea si instalarea datelor de activare58
5.1.1.4.2. Protectia datelor de activare58
5.1.1.4.3. Alte aspecte cu privire la datele de activare58
5.1.2. Masuri de securitate fizica, procedurala, de personal si a documentelor58
5.1.2.1. Controale de securitate fizica59
5.1.2.1.1. Accesul fizic59
5.1.2.1.2. Energie si climatizare60
5.1.2.1.3. Expunerea la apa60
5.1.2.1.4. Prevenirea si protectia impotriva incendiilor60
5.1.2.1.5. Mediile de stocare60
5.1.2.1.6. Aruncarea lucrurilor nefolositoare60
5.1.2.1.7. Depozitarea backup-urilor in afara locatiei61
5.1.2.2. Controale procedurale61
5.1.2.2.1. Functii de incredere61
5.1.2.2.2. Numarul de persoane necesare pentru fiecare sarcina63
5.1.2.2.3. Identificarea si autentificarea pentru fiecare rol63
5.1.2.3. Controale de personal64
5.1.2.3.1. Cerinte privind trecutul, calificarile si experienta64
5.1.2.3.2. Cerinte de pregatire65
5.1.2.3.3. Cerintele si frecventa cursurilor de perfectionare65
5.1.2.3.4. Sanctiuni pentru actiuni neautorizate66
5.1.2.3.5. Cerinte pentru contractarea personalului66
5.1.2.3.6. Documentatie furnizata personalului66
5.2. Controale CompuSEC66
5.2.1. Cerintele de securitate specifice66
5.2.2. Controale pentru managementul securitatii informatiei67
5.2.3. Controale de securitate a retelei67
5.3. Inregistrarea evenimentelor si procedurile de auditare68
5.4. Arhivarea inregistrarilor68

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.4.1. Tipurile de date arhivate69
5.4.2. Frecventa arhivarii datelor69
5.4.3. Perioada de pastrare a arhivelor70
5.4.4. Cerintele pentru marcarea temporala a inregistrarilor70
5.5. Procedura de backup si restaurare70
5.6. Compromiterea securitatii cheii si recuperarea in caz de dezastru70
5.6.1. Compromiterea resurselor de calcul, a aplicatiilor software si/sau datelor71
5.6.2. Compromiterea sau suspiciunea compromiterii cheii private a unei Autoritati de Certificare71
6. Profilele certificatelor, a listei de revocare a certificatelor si a protocolului de verificare on-line a starii certificatului72
6.1. Profilul certificatelor72
6.1.1. Continutul certificatului72
6.1.1.1. Campurile de baza72
6.1.1.2. Extensiile standard ale certificatelor73
6.1.2. Identificatorul algoritmului de semnare75
6.1.3. Campul ce contine semnatura electronica75
6.2. Profilul listei de certificate revocate (CRL)75
6.2.1. Extensiile acceptate in intrarile din CRL76
6.3. Profilul raspunsului de confirmare OCSP76
6.3.1. Numarul versiunii77
6.3.2. Informatiile despre starea certificatului77
6.3.3. Extensiile standard acceptate77
7. Managementul DPSI77

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

1. Introducere

Acest document constituie Declaratia practicilor aplicabile serviciilor de incredere furnizate de Alfatrust (numit in continuare prescurtat si DPSI) al S.C. AlfaTrust Certification S.A.

Acest document descrie practicile si procedurile de lucru pe care Furnizorul de Servicii de Certificare AlfaTrust Certification ("FSC") le utilizeaza in furnizarea serviciilor de certificare, sigilii electronice si marcare temporala in conformitate cu prevederile reglementarilor legale nationale precum si a Regulamentului European Nr. 910/2014.

DPSI se aplica companiei AlfaTrust Certification S.A., ca Autoritate de Certificare (AC), Autoritate de Inregistrare (AI), Autoritate de Marcare Temporala (TSA) si Autoritate de Validare a certificatelor emise (AV), precum si oricaror AC-uri, AI-uri, TSA-uri sau AV-uri aflate in relatie de subordonate sau aflate in relatie contractuala cu AlfaTrust.

1.1. Rolul DPSI

Acest document prezinta si explica practicile si procedurile de lucru ale companiei AlfaTrust Certification S.A. continand printre altele:

- Indatoririle autoritatii de certificare, ale autoritatii de inregistrare, ale autoritatii de marcare temporala precum si ale utilizatorilor de certificate digitale, in special in cazul certificatelor calificate;
- Problemele legale referitoare la serviciile de incredere oferite de compania AlfaTrust Certification S.A.;
- Revizuirea practicilor de securitate si audit la care se supune compania AlfaTrust Certification S.A.;
- Metodele folosite pentru a confirma identitatea solicitantilor serviciilor;
- Procedurile operationale pentru serviciile de incredere, realizate de S.C. AlfaTrust Certification S.A; solicitari cu privire la emiterea, aprobarea, revocarea si reinnoirea certificatelor;
- Procedurile de securitate operationala pentru inregistrarile de verificare, retinerea rapoartelor si recuperarea dupa dezastru utilizate in cadrul S.C. AlfaTrust Certification S.A;
- Practicile de securitate fizica, de personal, de management al cheilor si de securitate logica ale S.C. AlfaTrust Certification S.A.;
- Lista de certificate emise, precum si lista de certificate revocate detinute de S.C. AlfaTrust Certification S.A,
- Administrarea DPSI, inclusiv metode de imbunatatire.

1.2. Servicii de incredere

S.C. AlfaTrust Certification S.A. ofera certificate (simple si/sau calificate), marci temporale si sigilii electronice AlfaTrust Certification™ pentru orice tip de utilizator, in limita legilor in vigoare.

Certificatele simple (necalificate) AlfaTrust Certification™ pot fi utilizate pentru autentificarea utilizatorului, semnatura electronica (***neopozabila in justitie***) si criptare (schimbul de chei simetrice).

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Certificatele calificate AlfaTrust Certification™ pot fi utilizate pentru autentificare, semnatura electronica extinsa (bazata pe certificat calificat – ***opozabila in justitie***), autentificare servere Web, criptare, pentru gateway-uri VPN, toate impreuna sau separat (in functie de serviciul ales de beneficiar) ca dovada a identitatii in orice tip de tranzactii electronice.

Certificatele furnizeaza siguranta identitatii utilizatorului pe baza prezentei fizice a acestuia in fata unei persoane care ii confirma identitatea, folosind cel putin o forma de identificare recunoscuta de autoritati.

1.3. Privire de ansamblu asupra infrastructurii de certificare

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

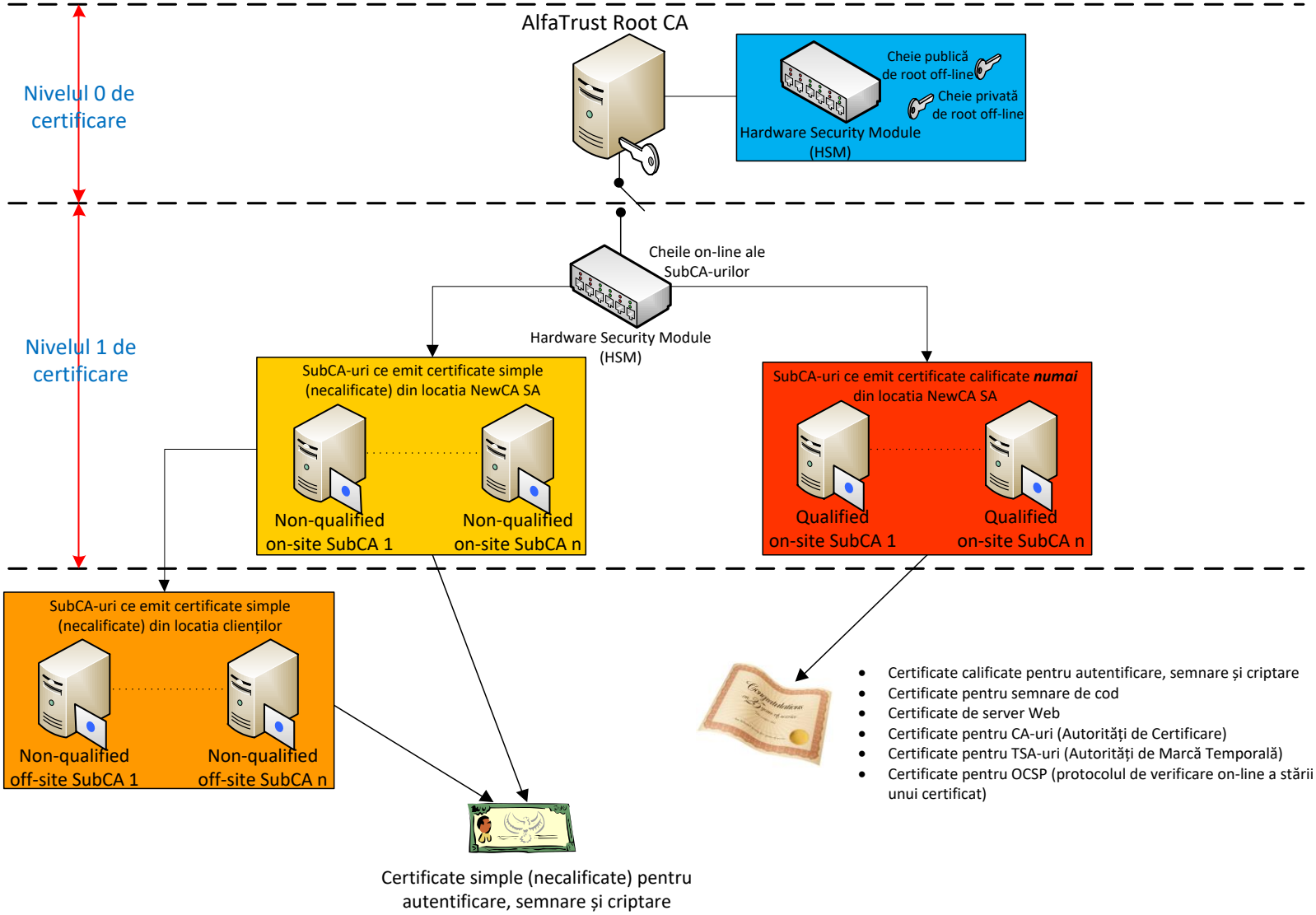
Nivelul 0 este format din AlfaTrust Certification ROOT CA. Autoritatile de certificare de pe nivelul 1 (on-site SubCA) sunt direct semnate de catre AlfaTrust Certification ROOT CA. Autoritatile de pe nivelul 2 (off-site SubCA – toate necalificate, ce emit doar certificate simple) sunt semnate de SubCA-uri necalificate on-site, si se afla plasate in locatia clientilor.

AlfaTrust Certification ROOT CA opereaza numai in mod off-line. In cazul compromiterii SubCA-urilor on-site, AlfaTrust Certification ROOT CA va fi folosita pentru a revoca certificatele acestora si pentru a emite noi certificate. In cazul compromiterii SubCA-urilor off-site, unul din SubCA-urile necalificat on-site va fi folosit pentru a revoca certificatele acestora si pentru a emite noi certificate.

Arhitectura Infrastructurii de Chei Publice (PKI) a AlfaTrust Certification este formata din doua ierarhii publice calificate, identice ca topologie. Ele difera doar prin algoritmul de semnare:

- ALFATRUST ROOT CA V2 – pentru emiterea de certificate si sigilii electronice semnate cu algoritmul SHA1.
- Alfasign Qualified Root CA – pentru emiterea de certificate si sigilii electronice semnate cu algoritmul SHA256.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro



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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

1.4. Sfera de aplicabilitate

1.4.1. Sfera de aplicabilitate a DPSI

Acest document se adreseaza tuturor participantilor, incluzand AlfaTrust Certification S.A., distribuitori, utilizatori finali persoane fizice sau juridice, entitati partenere si alte parti contractante. DPSI descrie practicile care guverneaza utilizarea certificatelor calificate AlfaTrust Certification™. Utilizatorilor de servicii AlfaTrust Certification™ li se permite sa foloseasca certificate emise pentru aplicatii de mare securitate care sunt descrise in DPSI.

Certificatele calificate AlfaTrust Certification™ destinate utilizatorilor permit tertilor (entitatilor partenere), participanti in procesul de comunicare electronica sa verifice semnaturile digitale bazate pe certificatele emise de AlfaTrust Certification.

Supusa legilor in vigoare, o semnatura digitala sau o tranzactie interactionand cu certificatul calificat AlfaTrust Certification™ va fi valid indiferent de locul in care certificatul calificat AlfaTrust Certification™ este emis sau de locul unde semnatura digitala a fost creata sau utilizata si indiferent de locul unde AC-ul sau utilizatorul isi desfasoara activitatea.

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

S.C. AlfaTrust Certification S.A. sau ceilalti participanti nu sunt responsabili pentru monitorizarea sau impunerea vreunei restrictii in aceste medii.

Cu toate acestea, anumite certificate calificate AlfaTrust Certification™ au functii limitate. De exemplu, certificatele ACP (Autoritatile de Certificare Primare) nu pot fi utilizate pentru alte functii decat cele de ACP. Mai mult, certificatele pentru client se supun aplicatiilor clientului si nu pot fi folosite ca certificate de server.

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

- **autentificare, semnare si criptare** (atat pentru certificatele simple cat si pentru cele calificate)
- **certificate de server, de semnare de cod, de AC, TSA si OCSP** – ca serviciu suplimentar, la cererea expresa a clientului (valabil doar pentru SubCA-urile ce emit certificate calificate).
- **sigilii electronice**.

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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

1.4.2. Sfera de aplicabilitate a certificatelor emise de AlfaTrust Certification

Sfera de aplicabilitate a certificatelor stabileste scopul in care poate fi folosit un certificat. Acest scop este definit de doua elemente:

- primul defineste aplicabilitatea certificatului (de exemplu, semnatura electronica, autentificare, criptare),
- celalalt este o lista sau o descriere a aplicatiilor permise sau interzise.

Certificatele emise de AlfaTrust Certification pot fi folosite preponderent pentru autentificare (utilizator sau masina), semnatura electronica si criptare, sau la cererea clientului se pot customiza extensiile astfel incat cerfificatele sa poata fi folosite si pentru semnare de cod, autentificare server Web, autentificare gateway-uri VPN avand doua nivele diferite de incredere.

Nivelul de sensibilitate al informatiilor ce se doreste a fi protejate trebuie evaluate de catre utilizatorul final, aceasta stand la baza deciziei de a folosi unul din tipurile de certificate furnizate de AlfaTrust Certification.

In prezentul document sunt definite doua nivele de incredere a certificatelor:

- **Certificate simple (necalificate)** = Pot fi folosite pentru autentificarea utilizatorului, semnatura electronica (dar nu semnatura electronica extinsa, in intelesul dat de legislatia in vigoare) si criptare. Acest nivel ofera o securitate de baza pentru informatii in medii cu grad scazut sau mediu de risc (risc fara consecinte majore). Dintre acestea, mentionam accesul la informatii private acolo unde probabilitatea de aparitie a unui acces neautorizat nu este foarte mare. Aceste certificate pot fi folosite pentru a autentifica si controla integritatea informatiei care a fost semnata si pentru a asigura confidentialitatea informatiei, mai ales in cazul postei electronice.
- **Certificate calificate** = Certificatul calificat reprezinta un certificat care satisface conditiile prevazute de legislatia in vigoare si care este eliberat de un furnizor de servicii de certificare ce satisface conditiile legale in materie. Aceste certificate pot fi utilizate pentru autentificare, creare de semnaturi electronice extinse, autentificare servere Web, autentificare gateway-uri VPN. Semnatura electronica extinsa (care este bazata doar pe un certificat ***calificat***) reprezinta acea semnatura electronica care indeplineste cumulativ reglementarile legale in vigoare.

  Acest nivel se recomanda pentru asigurarea securitatii informatiei in medii unde exista riscul aparitiei de brese de securitate iar consecintele acestor brese sunt moderate sau mari. Certificatele pot fi folosite pentru protectia tranzactiilor financiare sau a tranzactiilor in care exista sanse de aparitie a fraudelor. Aceste certificate pot fi folosite pentru protectia tranzactiilor de valoare nelimitata (daca nu se specifica altceva in certificat), a tranzactiilor in care exista mari sanse de aparitie a fraudelor.

AlfaTrust Certification emite mai multe tipuri de baza de certificate avand arii diferite de aplicabilitate dupa cum urmeaza:

- certificate simple pentru autentificare, semnare si criptare – permit semnarea e-mailurilor si fisierelor, sau autentificarea unui utilizator (de exemplu prin protocolul SSL);
- certificate calificate – permit autentificarea utilizatorului, criptarea mesajelor si semnarea documentelor cu valoare juridica;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- certificate pentru autentificarea serverelor si schimb de chei simetrice – sunt folosite de serviciile care opereaza pe baza protocoalelor SSL/TLS/WTLS;
- certificate pentru semnarea codului – folosite de programatori pentru a proteja software-ul impotriva falsificarii;
- certificate pentru Autoritatile de Certificare – folosirea lor nu este restrictionata la aria definita; aria de aplicabilitate poate fi data de extensia din certificate ce stabileste modul in care poate fi folosita cheia privata, sau de rolul acesteia (de exemplu, utilizator final, Autoritate de Certificare sau alta autoritate care furnizeaza servicii PKI); acest tip contine de asemenea si certificatele operationale ale Autoritatilor de Certificare;
- certificate pentru confirmarea starii unui certificat – sunt emise pentru serverele care functioneaza conform protocolului OCSP si care furnizeaza informatii despre starea certificatelor;
- certificate pentru Autoritati de Marcare Temporala – sunt emise serverelor care, ca raspuns la cererea unui utilizator al serviciului de time-stamping, emit marci temporale prin care asociaza unor date (documente, mesaje, semnaturi electronice etc.) un moment de timp pe baza caruia se poate determina secventialitatea in timp a datelor.
- sigilii electronice (certificate pentru sigilii electronice) – permit autentificarea entitatilor si semnarea documentelor cu valoare juridica;

Certificatele emise in concordanta cu politicile de certificare AlfaTrust Certification pot fi folosite in aplicatii ce satisfac cel putin urmatoarele conditii:

- gestioneaza corespunzator cheile publice si private,
- certificatele si cheile publice asociate acestora sunt folosite in concordanta cu scopul declarat al acestora, confirmat de catre AlfaTrust Certification,
- dispun de mecanisme interne de verificare a starii certificatelor, de creare a cailor de certificare si controlul validitatii (validitatea semnaturii, data expirarii etc.),
- ofera utilizatorului informatii corespunzatoare despre certificate si starea acestora.

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

Aplicatiile sunt incluse in lista aplicatiilor recomandate pe baza unor declaratii scrise ale producatorilor si/sau pe baza testelor facute de AlfaTrust Certification. AlfaTrust Certification permite fiecarui utilizator final sa-si genereze singur cheile criptografice folosite in procesul de certificare prin intermediul dispozitivelor recomandate. Autoritatea de Certificare poate, de asemenea, sa genereze cheile pe un dispozitiv criptografic si apoi sa livreze utilizatorului final dispozitivul impreuna cu cheile. In acest caz, AlfaTrust Certification foloseste dispozitive criptografice ce satisfac cel putin cerintele standardului FIPS PUB 140-2.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

1.4.3. Autoritati de certificare (AC)

Termenul autoritate de certificare cuprinde toate entitatile care emit certificate respectand propriul set de practici si proceduri, care poate fi acelasi pentru fiecare ACP, sau poate diferi de la un ACP la altul, in functie de scopul ACP-ului. Termenul “ACP” se refera la o subcategorie de emitenti numite autoritati de certificare primare (ACP), care se comporta ca radacini (eng. root). Fiecare ACP este o entitate AlfaTrust Certification™. Subordonate ACP-ului sunt autoritatile de certificare, care emit certificate abonatilor-utilizatori finali sau altor AC-uri. Toate ACP-urile AlfaTrust Certification™ ce emit certificate calificate sunt gazduite de centrul de procesare propriu, aflat pe teritoriul Romaniei, in locatiile strict securizate.

Autoritatea de Certificare AlfaTrust Certification ROOT CA (SHA1 sau SHA256) reprezinta punctul de incredere pentru clientii AlfaTrust Certification. Prin urmare, fiecare cale de certificare trebuie sa inceapa cu certificatul autoritatii AlfaTrust Certification ROOT CA (ALFATRUST ROOT CA V2 pentru SHA1 sau Alfasign Qualified Root CA pentru SHA256).

Autoritatea de Certificare Primara AlfaTrust Certification ROOT CA poate inregistra in depozitul de la nivelul Autoritatii de Validare si emite certificate numai Autoritatilor de Certificare Subordonate (numite de acum incolo SubCA-uri si care vor avea in nume AlfaSign).

Inainte de a incepe activitatea, fiecare autoritate de certificare subordonata (SubCA) trebuie sa trimita o cerere catre Autoritatea de Certificare Principala AlfaTrust Certification ROOT CA pentru inregistrare si emitere de certificat de cheie publica. Autoritatea AlfaTrust Certification ROOT CA functioneaza pe baza unui certificat autosemnat, emis de ea insasi. Intr-un astfel de certificat, extensia **certificatePolicies** lipseste, ceea ce semnifica faptul ca nu exista limitari ale setului de cai de certificare la care certificatul AlfaTrust Certification ROOT CA poate fi atasat.

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

- sine (emite si reinnoieste certificate proprii),
- Autoritatile de Certificare inregistrate in domeniul de certificare AlfaTrust Certification,
- entitati ce furnizeaza servicii de verificare on-line a starii certificatelor si ale entitatilor ce ofera servicii de non-repudiere (de exemplu, servicii de marcare temporala).

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

- utilizatori care vor sa-si asigure securitatea si credibilitatea postei electronice si a altor servicii (de exemplu, comert electronic, semnarea codului software) prin intermediul certificatelor,
- entitati care ofera servicii de marcare temporala,
- furnizori de servicii din domeniul telecomunicatiilor mobile,
- dispozitive de retea care realizeaza conexiuni criptate prin VPN,
- utilizatori in vederea oferirii de servicii pe baza de certificate de chei publice cum ar fi serviciul de verificare on-line a starii certificatelor (OCSP),
- alte Autoritati de Certificare,
- Sigilii electronice.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

1.4.4. Autoritati de inregistrare (AI)

AI-ul asista un AC prin indeplinirea functiilor de confirmare a identitatii, de aprobare sau respingere a cererilor pentru certificat, de cerere a revocarii certificatelor si de aprobare sau respingere a cererilor de reinnoire.

Nivelul de precizie al procesului de determinare a identitatii clientului este dat de nevoile utilizatorului final si este impus de nivelul certificatului pe care il solicita.

In cazul celei mai simple identificari, Autoritatea de Inregistrare verifica doar corectitudinea adresei de e-mail trimisa. Cea mai precisa identificare presupune prezenta in persoana a solicitantului la Autoritatea de Inregistrare si furnizarea de dovezi cu privire la identitatea sa.

Identificarea poate fi realizata fie automat (in cazul certificarii identitatii persoanei de catre o autoritate cu competente in acest sens conform legilor din Romania), fie manual de catre un operator al Autoritatii de Inregistrare (in cazul prezentarii viitorului utilizator final la sediul AlfaTrust Certification).

Toate AI-urile AlfaTrust Certification™ care asista ACP-urile AlfaTrust Certification™ la emiterea de certificate abonatilor-utilizatori finali sunt gazduite in propriile locatii securizate.

1.4.5. Autoritatea de Marcare Temporala (TSA)

Prin indeplinierea reglementarilor aferente Regulamentului (UE) nr. 910/2014 si ale Legii nr. 451/2004 privind marca temporala si a normelor sale aplicabile, AlfaTrust Certification S.A. isi defineste cadrul de a furniza servicii de marcare temporala catre abonati si isi asuma raspunderea deplina asupra furnizarii acestor servicii.

Alfatrust Certification S.A. primește cererile de marcare temporala si semneaza marcile temporale folosind serverul propriu de marcare temporala (Time Stamp Authority).

Sistemul informatic implementat de catre Alfatrust Certification S.A. permite furnizarea continua a serviciilor de marcare temporala si asigura faptul ca este imposibil sa fie emisa o marca corecta pentru un alt timp decat momentul cand a fost primita cerea de marcare temporala sau sa se schimbe ordinea in care marcile de timp sunt emise.

1.4.6. Autoritatea de Validare (AV)

Autoritatea de Validare este punctul in care Autoritatea de Certificare depoziteaza certificatele generate si lista de certificate revocate (urmare a cererilor primite prin intermediul Autoritatii de Inregistrare). Tot Autoritatea de Validare este responsabila de generarea raspunsului la interogarile primite prin OCSP (protocolul de verificare online a starii certificatelor).

Autoritatea de Validare AlfaTrust Certification se afla in locatia securizata a AlfaTrust Certification S.A.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

1.4.7. Utilizatorii finali si entitatile partenere

Un utilizator final este o entitate al carei identificator este plasat in campul Subject al unui certificat si care nu emite certificate altor entitati.

O Entitate Partenera este o entitate care foloseste certificatul unui utilizator final pentru a verifica semnatura electronica a acestuia sau pentru a asigura confidentialitatea informatiilor transmise.

Orice persoana fizica sau juridica, precum si dispozitivele hardware pe care acestea le detin pot fi utilizatori finali ai serviciilor oferite de AlfaTrust Certification, in conditiile respectarii legii. In particular, operatorii Autoritatii de Inregistrare, ceilalti angajati AlfaTrust Certification si echipamentele indispensabile pentru asigurarea securitatii infrastructurii AlfaTrust Certification (firewall-uri, routere, servere de autentificare) reprezinta, de asemenea, utilizatori finali.

Organizatiile (utilizatorii finali persoane juridice) care doresc sa obtina certificate emise de AlfaTrust Certification S.A. pentru angajatii lor, pot sa o faca prin intermediul reprezentantilor lor, pe cand utilizatorii finali persoane fizice trebuie sa ceara personal un certificat.

AlfaTrust Certification emite certificate de tipuri diferite si de niveluri de incredere diferite. Utilizatorii finali trebuie sa decida ce tip de certificat este cel mai potrivit pentru nevoile lor.

O Entitate Partenera poate fi orice entitate ce utilizeaza serviciile AlfaTrust Certification si care ia decizii bazandu-se pe corectitudinea legaturii dintre identitatea unui utilizator final si cheia sa publica (legatura confirmata de una din Autoritatile de Validare AlfaTrust Certification).

1.5. Detalii de contact

Intrebari despre prezenta Declaratia practicilor aplicabile serviciilor de incredere furnizate de Alfatrust Certification S.A. pot fi adresate la urmatoarea adresa:

S.C. AlfaTrust Certification S.A.

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

E-mail: office@AlfaSign.ro

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2. Dispozitii generale

2.1. Obligatii

2.1.1. Obligatiile Autoritatii de Certificare (AC)

S.C. AlfaTrust Certification S.A. face eforturi continue ca sa asigure buna legatura dintre serviciile oferite utilizatorilor finali si entitatilor partenere, ambii constituindu-se in parti contractante, obligatiile ambelor parti fiind stipulate clar si fara echivoc in cadrul contractului dintre parti in spiritul prezentei DPSI.

O Autoritate de Certificare (AC) care emite certificate, asumandu-si politica de certificare aflata in mod public la dispozitia utilizatorului final in vederea consultarii, are urmatoarele obligatii principale:

1. Crearea unui document care sa reflecte clar modalitatile de lucru, procedurile aplicabile si aplicate, politica generala a firmei, obligatiile si drepturile partilor contractante, etc. - DPSI (Declaratia practicilor aplicabile serviciilor de incredere furnizate de Alfatrust Certificaton) si afisarea lui in mod public (pe Internet) dupa ce a fost aprobat de persoanele responsabile din cadrul AC-ului;
2. Modul de desfasurare a activitatii AC-ului sa se conformeze strict cu prevederile DPSI-ului aprobat;
3. Modalitatea de punere in practica a DPSI-ului si a politicilor de certificare ale AC-ului sa se bazeze pe o infrastructura (de comunicatii, software si hardware) fiabila, capabila in orice moment de a garanta buna desfasurare a activitatii AC-ului conform cu politica de functionare 24x7 impusa nu numai de legile romanesti in vigoare privind Autoritatile de Certificare ce emit certificate calificate, dar si de realitatile actuale in ceea ce priveste afacerile desfasurate pe Internet;
4. Garantarea faptului ca cererile de emitere de certificate sunt procesate (in sensul identificarii persoanei numai pe baza modalitatilor puse la dispozitie de legile in vigoare) numai de o AI aflata in legatura contractuala cu AC-ul emitent de certificate (si caruia i se subordoneaza), si care la randul ei se conformeaza cadrului general stabilit de prezenta DPSI, in stransa legatura si cu documentul ce statueaza politica de certificare a AC-ului;
5. Garantarea faptului ca activitatea AI-ului pe linia identificarii persoanelor ce se inregistreaza in vederea obtinerii unui certificat digital calificat se desfasoara in litera si spiritul Legii nr. 677/ 2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date;
6. Garantarea faptului ca informatiile incluse in certificate sunt valide si conform realitatii la momentul aprobarii certificatului;
7. Garantarea aducerii la cunostinta utilizatorilor a obligatiilor pe care le au in concordanta cu aceasta DPSI, prin prisma faptului ca sunt posesori si virtuali utilizatori ai certificatelor digitale calificate, precum si informarea acestora asupra riscului la care se supun prin nerespectarea acestor obligatii;
8. Revocarea certificatelor acelor utilizatori despre care s-a stabilit (sau exista dubii) ca au actionat contrar obligatiilor ce revin utilizatorilor, asa cum se desprind ele din aceasta DPSI, cu obligativitatea AC-ului de a anunta utilizatorul despre masura luata;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

9. Serviciile de inregistrare in vederea emiterii de certificate si de ridicare a certificatelor in urma aprobarii acestora, servicii ce sunt destinate utilizatorului final trebuie sa fie furnizate exclusiv prin mijloace electronice, bazate pe o infrastructura care sa permita rularea acestora pe Internet (iar in cazuri particulare pe Intranet), cu obligativitatea AC-ului de a mentine un registru de evidenta a certificatelor emise de catre toate ACP-urile subordonate, registru ce trebuie actualizat dinamic astfel incat el sa reflecte situatia la zi a certificatelor emise catre abonati;

2.1.2. Obligatiile Autoritatii de Inregistrare (AI)

AI consta intr-un centru de procesare unde se garanteaza indeplinirea functiilor de validare, de aprobare sau respingere a cererilor pentru certificat prin cererea revocarii certificatelor si prin aprobarea cererilor de reinnoire. In prevederile DPSI sunt specificate obligatiile AI AlfaTrust Certification S.A.

O AI care realizeaza functii de inregistrare se va conforma prevederilor acestei DPSI. AC-urile sunt responsabile pentru asigurarea faptului ca certificatele sunt generate si administrate in conformitate cu aceasta DPSI si cu politica de certificare a AC-ului, si ca functiile de generare, administrare si retragere a certificatelor sunt realizate numai de cei care inteleg cerintele politicii de certificare asociate si care sunt de acord sa le respecte. Cerintele de securitate impuse AC-urilor sunt asemanatoare celor impuse oricaror AI-uri datorita faptului ca AI-urile sunt responsabile pentru informatia colectata. AI este responsabila cu:

1. Autentificarea entitatilor care solicita certificate digitale;
2. Validarea informatiilor furnizate de entitatile finale;
3. Validarea drepturilor entitatilor finale de a obtine certificate de un anumit tip;
4. Verificarea faptului ca entitatea finala detine intr-adevar cheia privata asociata cheii publice pentru care a solicitat un certificat digital. Acest proces este denumit in literatura de specialitate “dovada detinerii cheii private” (POP – Proof of Possession);
5. Distribuirea de chei si/sau certificate catre abonati;
6. Trimiterea de cereri catre AC pentru eliberarea, revocarea sau reinnoirea certificatelor;
7. Verificarea prealabila a datelor furnizate de abonati pentru aceste cereri, conform cerintelor din DPSI;
8. Asigurarea faptului ca PIN-ul si cheia privata ce urmeaza sa se distribuie catre abonat nu sunt interceptate de catre terte parti;
9. Transmiterea unui contract („Acordul Partilor”) ce urmeaza a fi semnat, catre fiecare utilizator ce urmeaza a fi detinatorul unui certificat.
10. Sa indice in mod clar utilizatorului ce tip de certificat digital (sau sigiliu electronic) va achizitiona.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.1.3. Obligatiile Autoritatii de Marcare Temporala (TSA)

Autoritatea de marcare temporala Alfatrust Certification isi atribuie o serie de obligatii fundamentale dupa cum urmeaza:

- Elaborarea unei politici de marcare temporala prin intermediul careia sa se defineasca modalitatea de lucru, procedurile aplicabile, obligatiile si drepturile partilor contractante, etc. care sa fie aprobat de catre Conducere si publicat intr-un mediu accesibil utilizatorilor carora i se adreseaza;
- Desfasurarea activitatii in conformitate cu procedurile descrise in prezentul document;
- Implementarea unor resurse hardware si software fiabile care sa sustina buna desfasurare a activitatii in mod permanent in baza reglementarilor impuse, dar si din punct de vedere al afacerilor in mediul virtual;
- Generarea unei perechi functionale cheie privata - cheie publica si protectia cheii private prin utilizarea unui dispozitiv criptografic securizat, cu adoptarea masurilor necesare pentru a preveni pierderea, dezvaluirea, modificarea sau utilizarea neautorizata a cheii private ce este folosita exclusiv in scopul aplicarii semnaturii electronice asupra marcilor temporale emise;
- Crearea si mentinerea un registru electronic operativ de evidenta a marcilor temporale incluzand momentul de timp la care au fost emise marcile temporale;
- Punerea la dispozitia utilizatorilor software-ul necesar pentru utilizarea serviciului de marcare temporala si informatiile legate de: conditiile in care este disponibil software-ul, instructiunile de folosire, obligatiile utilizatorului sau orice alte limitari privind utilizarea software-ului;
- Alocarea de personal ce detine cunostinte de specialitate, experienta si calificare necesare pentru furnizarea serviciilor de marcare temporala;
- Mentinerea pe o perioada de 10 ani a inregistrarilor marcilor temporale;
- Pastrarea documentatiei aferente algoritmilor si procedurilor de generare a marcilor temporale emise;
- Punerea la dispozitie a unui serviciu gratuit de verificare on-line a marcilor temporale;
- Asigurarea accesului permanent la baza de timp;
- In cazul incetarii activitatii, furnizorul de servicii de marcare temporala Alfatrust Certification se obliga sa transfere unui alt furnizor de servicii de marcare temporala sau, dupa caz, autoritatii registrul electronic operativ de evidenta, registrul marcilor temporale, precum si documentatia aferenta algoritmilor si procedurilor de generare a marcilor temporale emise.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.1.4. Obligatiile Autoritatii de Validare (AV)

Autoritatea de Validare AlfaTrust Certification contine trei componente principale:

1. Depozitul (repository), unde se tin toate certificatele impreuna cu datele lor de validare,
2. Lista Certificatelor Revocate (CRL), ce contine certificatele revocate pana la un moment bine stabilit de timp,
3. Protocolul de verificare online a starii certificatelor (OCSP), ce poate specifica in timp real daca un certificat este valabil sau nu.

Depozitul este gestionat si controlat de Autoritatea de Validare, prin urmare AlfaTrust Certification se obliga:

- sa depuna toate eforturile pentru a se asigura ca toate certificatele publicate in depozit apartin utilizatorilor finali inscrisi in certificate, iar utilizatorii si-au dat acordul asupra acestor certificate,
- sa se asigure ca certificatele Autoritatilor de Certificare apartinand domeniului AlfaTrust Certification precum si certificatele utilizatorilor (dupa aprobarea lor) sunt publicate si arhivate la timp,
- sa asigure publicarea si arhivarea Politicii de Certificare si Sigilii Electronice, a Politicii de Marcare Temporala a DPSI, a listei aplicatiilor si dispozitivelor recomandate,
- sa permita accesul la informatiile despre starea certificatelor prin publicarea de Liste de Certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogari HTTP,
- sa asigure accesul permanent la informatiile din depozit pentru Autoritatile de Certificare, Autoritatea de Inregistrare, utilizatori finali si Entitatile Partenere,
- sa publice CRL-urile sau alte informatii in timp util si in concordanta cu termenele limita specificate in Politica de Certificare si Sigilii Electronice,
- sa asigure accesul sigur si controlat la informatiile din depozit.

2.1.5. Obligatiile utilizatorului final

DPSI, Politica de Certificare si Sigilii Electronice si Politica de Marcare Temporala sunt parte integranta a fiecarui contract incheiat intre un utilizator final si AlfaTrust Certification. Prin aplicarea pentru inregistrare la Autoritatea de Inregistrare si semnarea confirmarii de inregistrare, utilizatorul este de acord sa se integreze in sistemul de certificare in conditiile statuate in documentele mentionate mai sus.

In functie de relatiile dintre AlfaTrust Certification si un abonat si de nivelul de credibilitate al certificatului solicitat de utilizator, obligatiile pot fi formulate sub forma unui contract intre abonat si AlfaTrust Certification.

Prin contract, utilizatorul final se angajeaza:

- sa fie de acord cu termenii contractului;
- sa aprobe fiecare certificat emis pentru el; garantiile si obligatiile AlfaTrust Certification in legatura cu un anumit tip de certificat sunt valide din momentul aprobarii certificatului de catre utilizator;
- sa ia masurile necesare care sa-i permita sa genereze in mod corespunzator (de catre el insusi sau de catre Autoritatea de Inregistrare) si sa stocheze in siguranta cheia privata din cadrul unei

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

perechi de chei (pentru a preveni pierderea, compromiterea, modificarea si folosirea neautorizata a acesteia);
- sa foloseasca dispozitivele si aplicatiile software recomandate de AlfaTrust Certification in cazul in care utilizatorul isi genereaza singur cheile;
- sa declare date corecte in aplicatiile trimise Autoritatii de Inregistrare care apoi sunt stocate in baza de date a AlfaTrust Certification si in certificate de chei publice emise; un utilizator trebuie sa fie constient de responsabilitatile ce ii revin pentru daunele directe si indirecte provocate ca urmare a falsificarii datelor;
- sa accepte faptul ca fiecare semnatura electronica creata prin intermediul unei chei private, apartinand utilizatorului si asociata unui certificat aprobat care contine cheia publica corespunzatoare, reprezinta semnatura utilizatorului si sa recunoasca faptul ca certificatul nu a fost invalid (in afara datei de valabilitate) si nici revocat sau suspendat atunci cand a fost creata semnatura;
- sa cunoasca in general notiunile referitoare la certificate, semnaturi electronice si PKI.

De asemenea, utilizatorul final se angajeaza:

- sa se supuna regulilor din DPSI, Politica de Certificare si Sigilii Electronice si Politica de Marcare Temporala
- sa genereze cheile criptografice, sa gestioneze parolele, cheile publice si private, sa schimbe informatii cu Autoritatea de Inregistrare si Autoritatile de Validare numai prin intermediul aplicatiilor software recomandate de catre AlfaTrust Certification; accesul la acest software, mediile si dispozitivele pe care sunt stocate cheile si parolele trebuie sa fie controlat in mod adecvat,
- sa considere pierderea sau dezvaluirea parolei (dezvaluirea parolei catre o persoana neautorizata) ca o pierdere sau dezvaluire a cheii private (dezvaluirea acesteia catre o persoana neautorizata),
- sa nu permita accesul la cheile sale private persoanelor neautorizate,
- sa nu foloseasca ca utilizator final o cheie privata asociata unui certificat emis de AlfaTrust Certification, pentru semnarea de CRL-uri sau certificate,
- sa faca dovada posesiei cheii private la Autoritatea de Inregistrare sau Validare sau sa demonstreze posesia acesteia in alt mod,
- sa nu dezvaluie parolele persoanelor neautorizate,
- sa transmita Autoritatii de Inregistrare documentele cerute care sa confirme informatiile incluse in aplicatia trimisa si identitatea celui ce a transmis cererea sau a entitatii ce actioneaza in numele utilizatorului,
- in cazul in care se constata incalcarea securitatii (sau exista suspiciunea de incalcare a securitatii) cheilor private, sa anunte emitentul certificatului ,
- sa foloseasca certificatele de chei publice si cheile private corespunzatoare numai in scopurile declarate in certificat si in concordanta cu ariile de aplicabilitate si restrictiile stabilite prin DPSI,
- sa obtina certificate de chei publice ale Autoritatilor de Certificare si Autoritatii de Inregistrare precum si cele corespunzatoare altor servicii oferite de AlfaTrust Certification.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.1.6. Obligatiile entitatilor partenere

DPSI, Politica de Certificare si Sigilii Electronice si Politica de Marcare Temporala sunt parte integranta a fiecarui contract incheiat intre AlfaTrust Certification, o entitate partenera si / sau un utilizator. Obiectul unui astfel de contract poate fi:

- furnizarea de servicii tip depozit, servicii de marca temporala si servicii de verificare a starii certificatelor (OCSP) – in cazul incheierii de contracte cu AlfaTrust Certification;
- specificarea conditiilor pe care trebuie sa le indeplineasca o semnatura electronica pentru a fi considerata valida de catre o entitate partenera – in cazul incheierii de contracte cu un utilizator;

In functie de relatiile dintre o entitate partenera si AlfaTrust Certification sau un abonat si de nivelele certificatelor acceptate de o entitate partenera, obligatiile entitatilor partenere sunt stabilite in cadrul unui contract incheiat intre AlfaTrust Certification si entitatea partenera.

Prin contract, Entitatea Partenera se angajeaza:

- sa fie de acord si sa respecte termenii si conditiile din contract. Drepturile si obligatiile partilor incep sa isi produca efectele incepand cu data incheierii contractului.
- sa verifice cu atentie fiecare semnatura electronica de pe un certificat sau document receptionat. Pentru a verifica semnatura, entitatea partenera trebuie:

i. sa specifice calea de certificare ce contine toate certificatele Autoritatilor de Certificare care fac posibila verificarea semnaturii de pe certificatul semnatarului,
ii. sa se asigure ca, din perspectiva crearii semnaturii calea de certificare aleasa este cea mai buna; in unele cazuri, este posibil sa existe mai mult de o cale pornind de la un certificat dat (prin intermediul caruia a fost creata semnatura) si pana la o Autoritate de Certificare pe care se bazeaza verificarea semnaturii,
iii. sa verifice ca nici unul din certificatele din calea de certificare, apartinand AlfaTrust Certification, nu se afla in listele de certificate revocate sau suspendate,
iv. sa verifice ca toate certificatele din calea de certificare apartin unor Autoritati de Certificare si ca acestea sunt autorizate sa semneze alte certificate,
v. (optional) sa specifice data si ora la care a fost semnat un document sau mesaj. Acest lucru este posibil numai daca documentul sau mesajul a fost marcat (inainte de semnare) cu o marca temporala emisa de o Autoritate de Marcare Temporala, sau semnaturii electronice i s-a asociat o marca temporala imediat dupa semnarea documentului; o astfel de verificare permite implementarea de servicii de non-repudiere sau se poate folosi pentru rezolvarea disputelor,
vi. sa verifice, folosind o cale de certificare definita, credibilitatea certificatului semnatarului documentului sau mesajului si autenticitatea semnaturii,

- sa efectueze corect operatiile criptografice, folosind aplicatii software si dispozitive avand un nivel de securitate corespunzator nivelului de sensibilitate al certificatului procesat si nivelului de credibilitate al certificatelor folosite,
- sa considere o semnatura electronica ca fiind invalida daca prin mijloacele software sau dispozitivele folosite nu este posibil sa se determine daca semnatura electronica este valida sau daca rezultatul verificarii este negativ,
- verificarea semnaturii electronice isi propune sa stabileasca daca:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

1. semnatura electronica a fost creata prin intermediul unei chei private corespunzatoare unei chei publice dintr-un certificat emis de AlfaTrust Certification pentru un utilizator final si
2. mesajul (documentul) semnat nu a fost modificat dupa semnare.

- sa aiba incredere numai in acele certificate de chei publice care:
  1. sunt folosite in concordanta cu scopul declarat si corespund ariilor de aplicabilitate specificate de entitatea partenera, de exemplu, printr-o politica de semnatura,
  2. a caror stare a fost verificata pe baza Listelor de Certificate Revocate (CRL) corespunzatoare, sau prin intermediul serviciului OSCP al AlfaTrust Certification.
- sa specifice conditiile pe care un certificat de cheie publica si o semnatura electronica trebuie sa le indeplineasca pentru a fi considerate valide; aceste conditii pot fi formulate, de exemplu, sub forma unor politici de certificare acceptate si apoi publicate.

Orice document cu o semnatura electronica eronata, sau dubioasa trebuie sa fie respins sau supus altor proceduri care ar putea permite determinarea validitatii sale. Orice persoana care aproba un asemenea document poarta responsabilitatea pentru consecintele ce decurg din acest fapt.

Entitatea partenera trebuie sa ia la cunostinta prevederile DPSI si ale politicilor de certificare si de marcare temporala.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.2. Responsabilitati

2.2.1. Responsabilitatea Furnizorului de Servicii de Certificare (FSC)

Alfatrust Certification, in calitate de furnizor de servicii de incredere (servicii de certificare, sigilii electronice si marcare temporala), este raspunzator pentru prejudiciul adus oricarei persoane care isi intemeiaza conduita pe efectele juridice ale certificatelor, si anume:

a) in ceea ce priveste exactitatea, in momentul eliberarii certificatului, a tuturor informatiilor pe care le contine;
b) in ceea ce priveste asigurarea ca, in momentul eliberarii certificatului, semnatarul identificat in cuprinsul acestuia detinea datele de generare a semnaturii corespunzatoare datelor de verificare a semnaturii mentionate in respectivul certificat;
c) in ceea ce priveste asigurarea ca datele de generare a semnaturii corespund datelor de verificare a semnaturii, in cazul in care furnizorul de servicii de certificare le genereaza pe amandoua;
d) in ceea ce priveste revocarea certificatului, in cazurile si cu respectarea conditiilor prevazute in legislatie

De asemenea, AlfaTrust Certification S.A. ca furnizor de servicii de certificare poate sa indice in cuprinsul unui certificat calificat restrictii ale utilizarii acestuia, precum si limite ale valorii operatiunilor pentru care acesta poate fi utilizat, cu conditia ca respectivele restrictii sa poata fi cunoscute de terti.

AlfaTrust Certification S.A. ca furnizorul de servicii de certificare nu va fi raspunzatoare pentru prejudiciile rezultand din utilizarea unui certificat calificat cu incalcarea restrictiilor prevazute in cuprinsul acestuia.

Garantiile si limitele responsabilitatii dintre o AI si AC care asista emiterea certificatelor pe de o parte, si utilizatorul respectiv, pe de alta parte, se supun si sunt guvernate de catre acordurile dintre acestia cu respectarea legilor in vigoare.

2.2.2. Responsabilitatea utilizatorului

Serviciile AlfaTrust Certification S.A. cer abonatilor sa garanteze ca:

- Fiecare semnatura digitala creata prin utilizarea cheii private corespunzatoare cheii publice din certificat este semnatura digitala a utilizatorului si ca certificatul a fost acceptat si este operational (nu este expirat sau revocat) la momentul in care semnatura digitala a fost creata;
- Nici o persoana neautorizata nu a avut acces la cheia privata a utilizatorului;
- Toate relatarile facute de utilizator in cererea pentru certificat sunt adevarate;
- Toate informatiile furnizate de utilizator si continute de certificat sunt adevarate;
- Certificatul este folosit exclusiv pentru scopul declarat, in concordanta cu DPSI;
- Utilizatorul este un utilizator final, nu un AC si nu foloseste cheia privata corespunzatoare cheii publice din certificat pentru semnarea digitala a oricarui certificat (sau orice alt format de cheie publica certificata) sau lista de revocare a certificatelor, ca AC sau in alta calitate.

Titularii de certificate sunt obligati sa solicite, de indata, revocarea certificatelor, in cazul in care:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- au pierdut datele de creare a semnaturii electronice;
- au motive sa creada ca datele de creare a semnaturii electronice au ajuns la cunostinta unui tert neautorizat;
- informatiile esentiale cuprinse in certificat nu mai corespund realitatii.

2.2.3. Responsabilitatea partilor contractante

Partile contractante admit ca au informatii suficiente pentru a lua o decizie in masura in care au ales sa se bazeze pe informatiile dintr-un certificat, ca sunt singurii responsabili pentru decizia de a se baza sau nu pe astfel de informatii, si ca vor suporta consecintele legale in cazul nerespectarii obligatiilor de catre parti.

2.3. Responsabilitati financiare

In masura limitelor legale, S.C. AlfaTrust Certification S.A. solicita abonatilor sa o despagubeasca in unul din urmatoarele cazuri:

- Falsitate sau relatare gresita in cererea pentru certificate;
- Relatarea gresita a unei informatii importante in cererea pentru certificat, daca relatarea gresita sau omisiunea a fost facuta din neglijenta sau cu intentia de a insela una dintre parti;
- Neprotejarea cheii private sau neluarea masurilor de protectie necesare prevenirii, compromiterii, pierderii, dezvaluirii, modificarii sau folosirii neautorizate a cheii private a utilizatorului;
- Utilizatorul a folosit un nume (inclusiv un nume comun, nume de domeniu sau adresa de e-mail), care incalca drepturile de proprietate intelectuala a unui tert.

AlfaTrust Certification S.A. va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfasurarii activitati de certificare persoanelor care isi intemeiaza conduita pe efectele juridice ale certificatelor calificate, pana la concurenta echivalentului in lei al sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat este fiecare prejudiciu produs, chiar daca se produc mai multe asemenea prejudicii ca urmare a neindeplinirii de catre furnizor a unei obligatii prevazute de lege.

2.4. Legea aplicabila si solutionarea litigiilor

Prevederile cuprinse in prezentul document se supun legii romane in materie, lege care guverneaza si interpretarea clauzelor cuprinse in acest document.

In situatia aparitiei unei neintelegeri intre partile contractante, acestea vor incerca solutionarea acestora in termen de 60 de zile de la notificarea transmisa de catre o parte catre cealalta parte (perioada de negociere initiala) si, in cazul in care partile nu ajung la o solutie acceptata de comun acord, acestea se pot adresa instantei de judecata competente.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.5. Pretul serviciilor prestate

Valoarea serviciilor de certificare si categoriile de servicii pentru care sunt percepute taxe sunt publicate in lista de preturi disponibila la adresa http://www.AlfaSign.ro.

Serviciile oferite de AlfaTrust Certification S.A. sunt stabilite dupa cum urmeaza:

a) **servicii de certificare individuale** – pretul este stabilit pentru fiecare serviciu in parte, de exemplu, pentru fiecare certificat vandut sau un numar mic de certificate,
b) **pachete de servicii de certificare** – pretul este stabilit pentru pachete de servicii prestate unei singure entitati,
c) **servicii prestate pe baza de abonament** – pretul este stabilit pentru servicii prestate lunar; valoarea sumelor platite depinde de tipul si numarul serviciilor accesate si este utilizat in special (dar nelimitandu-se la acestea) pentru serviciile de marcare temporala si de verificare a starii certificatelor prin intermediul protocolului OCSP,
d) **servicii indirecte** – pretul este stabilit pentru fiecare serviciu oferit clientilor sai de un partener AlfaTrust Certification S.A., care isi bazeaza activitatea pe infrastructura AlfaTrust Certification; de exemplu, daca o Autoritate de Certificare comerciala este certificata de AlfaTrust Certification, atunci AlfaTrust Certification va percepe un pret pentru fiecare certificat emis de Autoritatea de Certificare respectiva.

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

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

- vanzarea de dispozitive criptografice de orice tip, in functie de nevoile utilizatorului,
- generarea cheilor pentru Autoritatile de Certificare sau utilizatori,
- testarea aplicatiilor si includerea lor in lista aplicatiilor recomandate,
- vanzarea de licente,
- activitati de proiectare, implementare si instalare,
- activitati de consultanta si audit in domeniul securitatii informatiei,
- cursuri de instruire.

2.6. Publicarea si inregistrarea informatiilor

2.6.1. Publicarea informatiilor de catre AlfaTrust Certification S.A.

Depozitul (repository) este o interfata publica catre urmatoarele informatii:

- Versiunea curenta si cea anterioara a Politicii de Certificare si Sigilii Electronice, a Politicii de Marcare Temporala si a DPSI,
- Modelele de contract cu utilizatorii finali si Entitatile Partenere,
- Declaratia AlfaTrust Certification S.A. cu privire la asigurarea confidentialitatii informatiilor receptionate si procesate,
- Registrul (in acceptiunea Legii 455/2001 a semnaturii electronice),

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- Certificatul (sau certificatele) AlfaTrust Certification ROOT CA, precum si certificatele tuturor Autoritatilor de Certificare care apartin sau sunt legate la domeniul AlfaTrust Certification,
- Certificatele utilizatorilor finali (entitati fizice si juridice, inclusiv angajatii AlfaTrust Certification S.A. si masinile / aplicatiile software detinute de acestia si care sunt indispensabile pentru serviciile PKI) conform Legii 455/2001 a semnaturii electronice.

In plus, in Depozit se gasesc informatii legate de functionarea certificatelor, cum ar fi:

- Listele de certificate Revocate (CRL); CRL-urile sunt disponibile in asa numitele puncte de distributie a CRL-urilor, a caror adresa este specificata in fiecare certificat emis de AlfaTrust Certification; locatia principala de distributie a CRL-urilor este in depozit la adresa: http://www.AlfaSign.ro/.
- Alte informatii ce se modifica frecvent sau in timp real,

Continutul depozitului este disponibil prin Internet la adresa: http://www.AlfaSign.ro/.

2.6.2. Frecventa publicarii

Informatiile publicate de AlfaTrust Certification sunt actualizate cu urmatoarea frecventa:

- Politica de Certificare si Sigilii Electronice, Politica de Marcare Temporala si DPSI – la aprobarea initiala si ori de cate ori se modifica,
- certificatele Autoritatilor de Certificare din cadrul AlfaTrust Certification – dupa emiterea unui nou certificat,
- certificatul Autoritatii de Inregistrare – dupa emiterea unui nou certificat,
- certificatele Abonatilor – dupa fiecare emitere a unui nou certificat,
- Lista certificatelor Revocate – vezi Capitolul “frecventa de emitere a CRL-ului”,
- Rapoartele de audit efectuate de institutiile autorizate – in momentul in care AlfaTrust Certification intra in posesia lor,
- Informatiile suplimentare – dupa fiecare actualizare.

2.6.3. Controlul accesului la informatii

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

AlfaTrust Certification a implementat mecanisme logice si fizice de protectie impotriva adaugarii, stergerii si modificarii informatiilor publicate in depozit.

In momentul descoperirii unor brese ce afecteaza integritatea informatiilor din depozit, AlfaTrust Certification va lua masurile corespunzatoare pentru a restabili integritatea informatiilor, va trage la raspundere pe cei vinovati si va notifica entitatile afectate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

2.7. Evaluarea conformitatii

In conformitate cu prevederile art. 20, alin. (1) din Regulamentul (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna, Alfatrust Certification S.A. contracteaza o data la 24 de luni un organism de evaluare a conformitatii acreditat cu scopul de a confirma ca Alfatrust Certification, in calitate de prestator de servicii de incredere calificat si serviciile de incredere pe care le presteaza indeplinesc cerintele prevazute in Regulamentul (UE) nr. 910/2014

Aceste evaluari au ca obiectiv verificarea consistentei actiunilor AlfaTrust Certification sau a entitatilor delegate de aceasta cu declaratiile si procedurile acestora (inclusiv Politica de Certificare si Sigilii Electronice, Politica de Marcare Temporala si DPSI).

Auditurile desfasurate de AlfaTrust Certification urmaresc in principal centrele de procesare a datelor si procedurile de gestiune a cheilor. De asemenea, aceste audituri au in vedere si Autoritatile de Certificare de pe calea de certificare a AlfaTrust Certification ROOT CA, Autoritatea de Inregistrare sau alte elemente ale infrastructurii de chei publice, cum ar fi de exemplu serverele OCSP.

Evaluarea conformitatii se desfasoara conform regulilor si procedurilor acceptate pe plan international pentru furnizorii de servicii de incredere si vizeaza:

- securitatea fizica a AlfaTrust Certification,
- procedurile de verificare a identitatii utilizatorilor,
- serviciile de incredere si procedurile de furnizare a serviciilor,
- securitatea aplicatiilor software si a accesului la retea,
- securitatea personalului AlfaTrust Certification,
- jurnalele de evenimente si procedurile de monitorizare a sistemului,
- arhivarea si restaurarea datelor,
- procedurile de arhivare,
- inregistrarile referitoare la analizele si verificarile efectuate pentru aplicatiile software si dispozitivele hardware.

2.8. Confidentialitate

Toate informatiile pe care le detine AlfaTrust Certification S.A. au fost obtinute, pastrate si procesate in concordanta cu legile in vigoare, in mod special cu Legea romaneasca privind protectia datelor cu caracter personal (Legea 677/2001) si cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice. Relatiile dintre un utilizator, o entitate partenera si AlfaTrust Certification se bazeaza pe incredere.

O terta parte poate avea acces doar la informatiile disponibile public in certificate. Celelalte date furnizate in aplicatiile trimise catre AlfaTrust Certification nu vor fi dezvaluite in nici o circumstanta vreunei terte parti, in mod voluntar sau intentionat (cu exceptia situatiilor prevazute de lege).

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

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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Arhivarea cheilor de criptare se face doar la solicitarea expresa a clientului. AlfaTrust Certification nu arhiveaza niciodata cheile de semnare.

O parte va fi exonerata de raspunderea pentru dezvaluirea de informatii confidentiale, daca:

- informatia era cunoscuta partii contractante inainte ca ea sa fi fost primita de la cealalta parte contractanta; sau
- informatia a fost dezvaluita dupa ce a fost obtinut acordul scris al celeilalte parti pentru asemenea dezvaluire; sau
- partea a fost obligata in mod legal sa dezvaluie informatia.

Dezvaluirea oricarei informatii fata de persoanele implicate in indeplinirea obligatiilor, se va face confidential si se va extinde numai asupra acelor informatii necesare in vederea indeplinirii obligatiilor.

AlfaTrust Certification S.A., angajatii acesteia precum si entitatile care desfasoara activitati de certificare sunt obligate sa pastreze secretul informatiilor, atat pe durata, cat si dupa incetarea contractului de munca, in cazul angajatilor.

Sunt catalogate drept informatii private sau confidentiale:

- informatiile furnizate de utilizatori, in plus fata de informatiile ce trebuie transmise reevaluate pentru efectuarea serviciilor de certificare; in celelalte cazuri, dezvaluirea informatiilor primite necesita in prealabil o aprobare scrisa din partea proprietarului informatiei sau in alte conditii prevazute de lege,
- informatiile furnizate de, sau catre utilizatori (de exemplu, continutul contractelor incheiate cu utilizatorii finali sau Entitatile Partenere, conturi bancare, aplicatiile de inregistrare, emitere, reinnoire, revocare certificate – cu exceptia informatiilor incluse in certificate sau din depozit, conform prezentului document); o parte din informatiile mentionate mai sus poate fi dezvaluita doar cu aprobarea si in scopul mentionat de proprietarul informatiilor (de exemplu, utilizatorul),
- inregistrarile corespunzatoare tranzactiilor din sistem (toate tipurile de tranzactii, precum si datele pentru controlul tranzactiilor, asa numitele loguri ale tranzactiilor din sistem),
- inregistrarile corespunzatoare evenimentelor (loguri) ce tin de serviciile de certificare, pastrate de catre AlfaTrust Certification,
- rezultatele auditurilor interne si externe, daca acestea reprezinta o amenintare pentru securitatea AlfaTrust Certification,
- planurile in caz de urgenta,
- informatiile referitoare la masurile luate pentru protectia dispozitivelor hardware si aplicatiilor software, informatiile referitoare la modul de administrare a serviciilor de certificare si a regulilor de inregistrare planificate.

Obligatia de confidentialitate nu se rasfrange si asupra faptului ca AlfaTrust Certification a oferit servicii de certificare unei parti. Persoanele responsabile de pastrarea confidentialitatii informatiilor si care se supun regulilor referitoare la modul de gestiune a informatiilor poarta raspunderea penala conform legislatiei in vigoare.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

2.9. Drepturi de proprietate intelectuala

Toate marcile, patentele, siglele, licentele, imaginile grafice etc. folosite de catre AlfaTrust Certification S.A. sunt si vor ramane proprietatea intelectuala a detinatorilor legali ai acestora. AlfaTrust Certification S.A. se obliga sa specifice acest lucru conform cerintelor impuse de detinatori.

Toate marcile, patentele, siglele, licentele, imaginile grafice etc., apartinand AlfaTrust Certification S.A. sunt si raman proprietatea acesteia, indiferent daca sunt insotite sau nu de patente, modele de utilitate, copyright sau altele asemenea si nu pot fi reproduse sau furnizate unei terte parti fara acordul prealabil in scris al AlfaTrust Certification S.A.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

3. Identificare si autentificare

Acest capitol prezinta regulile generale pentru verificarea identitatii Abonatului, reguli care se aplica la emiterea de certificate de catre AlfaTrust Certification. Acestea au la baza anumite tipuri de informatii care sunt incluse in certificate si specifica mijloacele indispensabile pentru a se asigura ca informatia este precisa si credibila la momentul emiterii certificatului.

Verificarea este facuta in mod obligatoriu in etapa de inregistrare si de modificare a datelor utilizatorului precum si la cererea AlfaTrust Certification in cazul oricarui alt serviciu de certificare.

3.1. Inregistrarea initiala

Inregistrarea utilizatorului final are loc atunci cand un utilizator care cere inregistrarea nu detine un certificat valid emis de nici o Autoritate de Certificare afiliata la AlfaTrust Certification.

Fiecare utilizator este supus unui proces de inregistrare o singura data. Dupa verificarea datelor puse la dispozitie de un utilizator, acesta este inclus pe lista utilizatorilor autorizati ai serviciilor AlfaTrust Certification si i se acorda un certificat de cheie publica.

Fiecare utilizator care solicita servicii specifice infrastructurilor de chei publice si care cere emiterea unui certificat trebuie (inainte de emiterea certificatului) sa:

- completeze un formular de inregistrare 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 si sa furnizeze Autoritatii de Inregistrare dovada detinerii unei chei private; optional, utilizatorul poate sa insarcineze o Autoritate de Certificare sau Autoritatea de Inregistrare cu generarea acestei perechi de chei,
- sugereze un nume distinctiv (ND),
- completeze si sa trimita un formular de inregistrare care contine o cheie publica si dovada posesiei cheii private corespunzatoare acesteia,
- sa se prezinte, optional, la Autoritatea de Inregistrare si sa furnizeze documentele necesare (daca se cere acest lucru de politica de certificare pe baza careia se emite certificatul),
- incheie un contract cu un functionar al Autoritatii de Inregistrare in legatura cu furnizarea serviciilor de catre AlfaTrust Certification; prezenta DPSI este parte integranta a acestui contract.

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

3.1.1. Tipuri de nume

Certificatele emise de AlfaTrust Certification respecta standardul X.509 v3. Aceasta inseamna ca emitentul de certificate si Autoritatea de Inregistrare care actioneaza in numele emitentului aproba numele utilizatorului, conform standardului X.509 (cu referire la recomandarile seriei X.500). Numele de baza ale utilizatorilor si ale emitentilor de certificate plasati in certificatele AlfaTrust Certification sunt in concordanta cu Numele Distinctive – ND – (cunoscute si ca nume directoare), create respectand

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

recomandarile X.500 si X.520. In cadrul ND, este posibila definirea de atribute ale Domain Name Service (DNS). Aceasta permite utilizatorilor sa foloseasca doua tipuri de nume: ND si DNS simultan. Aceasta optiune este foarte importanta in cazul emiterii de certificate catre servere sub administrarea utilizatorului.

3.1.2. Necesitatea ca numele sa aiba sens

Numele incluse in Numele Distinctiv al utilizatorului trebuie sa aiba un sens in limba romana sau in alta limba care utilizeaza alfabet latin. Structura Numelui Distinctiv, aprobat / atribuit si verificat de o Autoritate de Inregistrare, depinde de tipul utilizatorului.

Pentru entitati private (persoane fizice sau angajati ai companiilor), ND consta din urmatoarele campuri, obligatorii sau nu (descrierea campului este urmata de abrevierea sa care respecta recomandarile RFC 3280 si X.520):

- **campul C** – abrevierea internationala pentru numele tarii (RO pentru Romania),
- **campul S** – judetul / sectorul in care locuieste utilizatorul,
- **campul L** – orasul in care utilizatorul are domiciliul,
- **campul Street** – adresa utilizatorului,
- **campul CN** – numele utilizatorului; numele unui produs sau echipament poate de asemenea sa fie specificat aici,
- **campul O** – numele institutiei in cadrul careia lucreaza utilizatorul, in cazul in care certificatul este emis catre o persoana juridica,
- **campul OU** – numele departamentului in care este angajat utilizatorul, in cazul in care certificatul este emis catre o persoana juridica,
- **campul T** – functia utilizatorului,
- **campul SN** – numele de familie al utilizatorului,
- **campul G** – prenumele utilizatorului,
- **campul P** – pseudonimul utilizatorului pe care acesta il foloseste in mediul sau, sau pe care doreste sa il foloseasca pentru a nu-si face public numele sau prenumele real,
- **campul Phone** – numarul de telefon,
- **campul Serial Number** – codul personal de identificare al utilizatorului in sensul Legii 455/201 a semnaturii electronice.

Pentru persoanele juridice, ND consta in urmatoarele campuri optionale (descrierea campului este urmata de abrevierea sa care respecta recomandarile X.520):

- **campul C** – abrevierea internationala pentru numele tarii (RO pentru Romania),
- **campul O** – numele institutiei,
- **campul OU** – numele departamentului organizatiei,
- **campul S** – judetul / sectorul in care functioneaza organizatia,
- **campul L** – orasul in care utilizatorul locuieste sau are domiciliu,
- **campul CN** – numele institutiei,
- **campul Phone** – numarul de telefon,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Numele utilizatorului trebuie confirmat de un operator al Autoritatii de Inregistrare si aprobat de o Autoritate de Certificare. AlfaTrust Certification asigura (in cadrul domeniului sau) unicitatea ND-urilor.

3.1.3. Unicitatea numelor

Interpretarea campurilor din certificatele emise de AlfaTrust Certification se face in concordanta cu profilele de certificate descrise in Profilul certificatelor si al CRL-urilor.

Identificarea fiecarui detinator de certificate emise de AlfaTrust Certification se realizeaza pe baza ND-ului. AlfaTrust Certification asigura unicitatea ND-ului asignat fiecarui utilizator.

ND-ul utilizatorului este sugerat de acesta in cererea sa. Daca numele este in concordanta cu cerintele generale specificate in subcapitolul 3.1.1 si 3.1.2, un operator al Autoritatii de Inregistrare accepta temporar sugestia. Daca operatorul Autoritatii de Inregistrare are acces la baza de date cu ND-uri, acesta va verifica si unicitatea numelui in domeniul AlfaTrust Certification. Daca testul confirma unicitatea, ND-ul este acceptat. In cazul lipsei accesului la baza de date a AlfaTrust Certification, decizia cu privire la acceptarea sau refuzul ND-ului se ia de catre operatorul Autoritatii de Certificare.

Daca un ND sugerat de utilizator incalca drepturile altor entitati la acest nume, AlfaTrust Certification poate adauga alte atribute ND-ului (ex. numarul serial), care asigura unicitatea acestui nume in cadrul domeniului AlfaTrust Certification.

Formatul numelui unic global pentru un utilizator are urmatoarea forma:

AlfaSign.ro / numele emitentului / numele utilizatorului

in care AlfaSign.ro este numele domeniului AlfaTrust Certification, numele emitentului este ND-ul uneia din Autoritatile de Certificare si numele utilizatorului este ND-ul campului *Subject* din certificat.

Valorile ultimelor doua campuri sunt extrase din certificat.

Daca un utilizator renunta la serviciile AlfaTrust Certification, eventuala cererea de atribuire a ND-ului sau altui utilizator va fi respinsa.

AlfaTrust Certification poate inregistra un utilizator cu un Nume Distinctiv folosit in trecut de alt utilizator numai cu acordul scris al acestuia din urma.

3.1.4. Procedura aplicabila in litigiile referitoare la dreptul la nume

Numele care nu apartin unui utilizator nu pot fi folosite in cererile sale de certificat. AlfaTrust Certification nu verifica daca un utilizator este indreptatit sa foloseasca numele mentionat in cererea de inregistrare si nici nu intentioneaza sa-si asume rolul de arbitru in rezolvarea disputelor privind drepturile de proprietate asupra oricarui Nume Distinctiv, marca comerciala sau nume comercial.

In disputele privind revendicarile de nume, AlfaTrust Certification este indreptatita sa respinga sau sa suspende cererea unui utilizator fara a-si asuma vreo responsabilitate in acest sens. AlfaTrust Certification este de asemenea indreptatita sa ia toate deciziile cu privire la sintaxa numelui unui utilizator si sa atribuie unui utilizator numele care rezulta ca urmare a acestor decizii.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

3.1.5. Autentificarea identitatii persoanelor juridice

Autentificarea identitatii unei persoane juridice se realizeaza pentru a dovedi ca, la momentul procesarii cererii, persoana juridica stipulata in cerere exista; de asemenea, este necesar sa se dovedeasca ca o persoana fizica solicitanta a unui certificat in numele societatii, sau care-l primeste este autorizata de catre aceasta persoana juridica sa o reprezinte.

Autentificarea identitatii unei persoane juridice se poate face fie prin prezenta personala a reprezentantului autorizat al persoanei juridice la Autoritatea de Inregistrare, fie prin prezenta in persoana a reprezentantului autorizat al Autoritatii de Inregistrare la sediul persoanei juridice (specificat in cerere).

Reprezentantii autorizati ai institutiei, indiferent de nivelul certificatului pe care il cer, sunt obligati sa prezinte, la cererea unui reprezentant al Autoritatii de Inregistrare, urmatoarele documente:

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

Procedura de verificare la AI a identitatii persoanei juridice si a identitatii reprezentantului sau autorizat consta in:

- verificarea documentelor furnizate de utilizator,
- verificarea cererii, care consta in:

i. verificarea conformitatii datelor mentionate in cerere cu cele din documentele furnizate,
ii. (optional) verificarea dovezii posesiei cheii private (daca cererea implica o pereche de chei pentru crearea unei semnaturi electronice) si masura in care Numele Distinctiv este cel potrivit,

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

Daca verificarile sunt incheiate cu succes, un operator autorizat al Autoritatii de Inregistrare:

- atribuie un nume distinctiv persoanei juridice sau aproba numele sugerat de aceasta prin inaintarea cererii,
- emite o confirmare prin care atesta conformitatea datelor din cererea in curs de procesare cu datele prezentate si trimite aceasta confirmare la Autoritatea de Certificare,
- face copii tuturor documentelor si certificatelor folosite de operator pentru verificarea identitatii persoanei juridice si identitatea reprezentantului sau care actioneaza in numele acesteia,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- in numele Autoritatii de Certificare, incheie un contract cu persoana juridica cu privire la prestarea serviciilor de certificare; contractul se incheie daca persoana juridica joaca rolul de utilizator, de Autoritate de Certificare, sau o entitate care presteaza alte servicii de certificare.

Confirmarea este trimisa Autoritatii de Certificare care verifica daca aceasta a fost emisa de o Autoritate de Inregistrare autorizata.

AlfaTrust Certification respinge cererea de inregistrare a unui solicitant daca descopera ca persoana juridica in cauza este deja inregistrata.

3.1.6. Autentificarea identitatii persoanelor fizice

Autentificarea identitatii persoanelor fizice (entitati private) are doua scopuri. Autentificarea trebuie sa dovedeasca

- ca datele dintr-o cerere se refera la o entitate privata existenta si
- ca solicitantul este intr-adevar entitatea privata mentionata in cerere.

Autentificarea persoanelor fizice se realizeaza pe baza documentelor personale (carte de identitate sau pasaport) care confirma identitatea solicitantului.

Procedura pentru persoanele fizice realizata in fata Autoritatii de Inregistrare consta in:

- verificarea documentelor furnizate de utilizator (carte de identitate sau pasaport in original sau copie legalizata), inclusiv bazele de date ale AC sau ale altor institutii,
- verificare cererii inaintate:
  - verificarea consecventei datelor din cerere cu cele din documente,
  - (optional) verificarea dovezii posesiei unei chei private si a gradului de potrivire a ND-ului.
- verificarea setului de informatii din cerere folosind alte surse (Registrul Comertului din Romania, Registrul de Evidenta a Populatiei etc.),
- verificarea faptului ca contul de mail care apare in cererea de certificat este controlat de catre abonat. Cererea de certificat nu poate fi facuta/validata in aplicatia software AI daca abonatul nu isi valideaza contul de email.

3.1.7. Autentificarea dispozitivelor

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

- identificatorul dispozitivului,
- cheia publica a dispozitivului,
- caracteristicile si autorizatiile dispozitivului (in cazul in care acestea trebuie specificate in certificat),
- datele de contact ale sponsorului, care sa permita Autoritatii de Inregistrare sau FSC-ului sa contacteze rapid sponsorul.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

3.2. Autentificarea identitatii la reinnoirea sau modificarea certificatului

Pentru a pastra continuitatea certificatului, inainte de expirarea sa, utilizatorul trebuie sa solicite un nou certificat. Noul certificat poate contine aceeasi cheie daca se respecta conditia ca durata de viata a cheilor sa nu depaseasca o durata de doua ori mai mare decat durata maxima de viata a unui certificat. In caz contrar se va emite un nou certificat.

Reinnoirea este permisa numai inainte de expirarea certificatului.

Identitatea utilizatorilor care cer reinnoirea certificatului, sau modificarea acestuia este verificata. Procedurile utilizate urmaresc verificarea faptului ca persoana sau organizatia care cer un nou certificat pentru un utilizator, sunt indreptatite la acest lucru.

Utilizatorii care trimit cereri direct la o Autoritate de Inregistrare vor fi verificati de aceasta autoritate pe baza semnaturii electronice si a certificatului cheii publice asociat cu aceasta semnatura.

3.2.1. Reinnoirea unui certificat

Un utilizator sau o Autoritate de Certificare foloseste reinnoirea daca detine deja un certificat si o cheie privata asociata acestuia. Noul certificat, creat ca rezultat al innoirii, va avea același Subject cu vechiul certificat. Perioada de valabilitate, numarul serial si semnatura emitentului sunt diferite fata de datele din certificatul anterior.

Reinnoirea se aplica numai certificatelor a caror perioada de validitate nu a expirat, nu au fost revocate si informatiile continute de acestea sunt intacte.

Fiecare cerere de reinnoire este procesata in mod off-line, adica necesita acceptarea manuala a operatorului Autoritatii de Certificare.

3.2.2. Modificarea unui certificat

Modificarea certificatului se refera la crearea unui nou certificat pe baza certificatului detinut in prezent de utilizator. Un nou certificat are o cheie publica diferita, un nou numar serial, dar difera prin cel putin un camp (prin continut sau prin aparitia unui camp complet nou) fata de certificatul pe baza caruia este emis. Modificarea poate fi necesara, de exemplu, in cazul schimbarii pozitiei in cadrul companiei sau al schimbarii numelui, cu conditia ca aceste date sa fi fost mentionate initial in certificat, sau daca trebuie adaugate. Daca datele, verificate pe baza unor documente in concordanta cu procedurile de autentificare ale utilizatorului au fost modificate, fiecare cerere trebuie confirmata de Autoritatea de Inregistrare. Pot fi modificate numai certificatele valide care nu au fost revocate si al caror nume al utilizatorului si alte caracteristici nu au fost schimbate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

3.3. Autentificarea identitatii la revocarea unui certificat

Cererile de revocare pot fi trimise prin e-mail direct emitentului certificatului sau indirect, Autoritatii de Inregistrare. Se pot trimite cereri si in alt format decat cel electronic.

- in primul caz, utilizatorul trebuie sa trimita o cerere autentificata pentru revocarea certificatului. Utilizatorul autentifica cererea aplicandu-i o semnatura electronica.
- Utilizatorul care a pierdut o cheie privata activa (sau i-a fost furata) trebuie sa foloseasca a doua metoda. Cererea de revocare trebuie sa fie certificata de Autoritatea de Inregistrare.

In ambele cazuri, trebuie sa existe o identificare fara echivoc a identitatii utilizatorului. Cererea de revocare poate sa vizeze mai multe certificate. Autentificarea si identificarea utilizatorului la Autoritatea de Inregistrare se realizeaza ca si la inregistrarea initiala.

Autentificarea utilizatorului la Autoritatea de Certificare consta in verificarea autenticitatii cererii. Procedura detaliata de revocare este descrisa in subcapitolul 4.3.

4. Cerinte operationale

In acest capitol sunt prezentate procedurile ce tin de procesul de certificare. Fiecare procedura incepe cu trimiterea, de catre utilizatorul final, a unei cereri: ***indirect*** (dupa confirmarea initiala a cererii de catre Autoritatea de Inregistrare) sau ***direct*** catre o Autoritate de Certificare. Pe baza cererii, Autoritatea de Certificare ia o decizie in legatura cu furnizarea / respingerea serviciului cerut.

Cererile trimise trebuie sa contina informatiile necesare pentru identificarea corecta a utilizatorului.

AlfaTrust Certification ofera acces la urmatoarele servicii de baza:

i. inregistrarea, certificarea, reinnoirea, modificarea de certificate;
ii. revocarea certificatelor;
iii. verificarea valabilitatii certificatelor.

Programul de lucru

Serviciile sunt oferite atat on-line, cat si la sediul firmei. Serviciile online sunt oferite permanent, iar cele de la sediul firmei, de luni pana vineri, intre orele 10 si 16. Pentru toate clasele de certificate serviciile de revocare a certificatelor sunt oferite in maxim 24 de ore de la solicitare.

4.1. Trimiterea cererii

Cererile pentru eliberarea unui certificat sunt trimise de utilizator catre Autoritatea de Inregistrare. Cererile sunt trimise prin protocoale de comunicatie precum HTTP, S/MIME sau TCP/IP. AlfaTrust Certification emite certificate numai pe baza cererilor de inregistrare, modificare sau reinnoire de certificate trimise de un utilizator final.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

4.1.1. Cererea de inregistrare

O cerere de inregistrare este trimisa de catre un utilizator final catre Autoritatea de Inregistrare si contine cel putin urmatoarele informatii:

i. numele complet al institutiei sau numele si prenumele utilizatorului final,
ii. numele distinctiv a carui structura depinde de categoria utilizatorului final,
iii. identificatori: Codul de Inregistrare al Firmei / Codul Numeric Personal
iv. adresa utilizatorului final,
v. tipul de certificat cerut,
vi. identificatorul politicii de certificare pe baza caruia este emis certificatul,
vii. adresa de e-mail,
viii. cheia publica care va fi certificata.

Ca urmare a autentificarii identitatii utilizatorului final si dupa primirea confirmarii Autoritatii de Inregistrare, cererea este trimisa unei Autoritati de Certificare.

4.1.2. Cererea de reinnoire sau modificare certificat

O cerere de modificare sau reinnoire certificat, trebuie sa contina cel putin:

i. numele distinctiv al solicitantului (utilizatorului final);
ii. tipul de certificat pe care-l solicita utilizatorul;
iii. identificatorul politicii de certificare pe baza careia trebuie emis certificatul;
iv. cheia publica (folosita anterior in cazul innoirii certificatului sau noua in cazul schimbarii de cheie de certificat) care va fi certificata.

4.1.3. Cererea de revocare a unui certificat

Informatiile incluse in cererea de revocare a unui certificat sunt urmatoarele:

i. numele distinctiv al solicitantului (utilizatorului final),
ii. lista de certificate de revocat sau suspendat, sub forma unei perechi: numarul serial, motivul revocarii.

Datele partiale sau complete incluse in cererea de mai sus trebuie autentificate prin semnatura electronica, daca utilizatorul detine o cheie privata valida pentru crearea de semnatura.

O cerere de revocare poate fi trimisa prin e-mail impreuna cu datele de autentificare, sub forma scrisa (scrisoare, fax), sau sub forma orala (telefon). In ultimele doua cazuri, certificatul este suspendat pana cand cererea va fi trimisa electronic.

In momentul suspendarii certificatului, operatorii Autoritatii de Inregistrare anunta utilizatorul final in legatura cu acest lucru.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

4.2. Tratarea cererilor de certificare

AlfaTrust Certification accepta cereri inaintate individual sau colectiv. Cererile pot fi trimise on-line si offline.

Cererea trimisa on-line se realizeaza prin intermediul paginilor web de pe serverul AlfaTrust Certification la adresa: https://www.AlfaSign.ro. Un utilizator care intra pe site-ul respectiv completeaza (conform instructiunilor de pe site) un formular de cerere si il trimite Autoritatii de Inregistrare a FSC-ului. Cererile pentru certificate simple (necalificate) sunt procesate automat, in timp ce cererile de certificate calificate sunt procesate manual.

Cererea trimisa off-line se poate face:

- Prin prezentarea in persoana a solicitantului sau a reprezentantului autorizat al companiei la Autoritatea de Inregistrare a Furnizorului de Servicii de Certificare (FSC), caz in care se completeaza si se semneaza de mana cererea, se semneaza contractul cu privire la prestarea serviciilor de certificare si se genereaza o parola cu ajutorul careia utilizatorul va putea face managementul certificatului sau se genereaza un cod PIN pentru accesul securizat la dispozitivul criptografic ce contine cheile si certificatele,
- Prin trimiterea prin posta a cererii si a copiilor documentelor necesare verificarii identitatii solicitantului; verificarea este urmata de generarea unei parole cu ajutorul careia utilizatorul va putea face managementul certificatului, sau generarea unui cod PIN pentru accesul securizat la dispozitivul criptografic ce contine cheile si certificatele; dispozitivul criptografic este trimis inapoi solicitantului (codul PIN este trimis separat).

4.2.1. La Autoritatea de Inregistrare (AI)

Fiecare cerere scrisa pe hartie este procesata dupa cum urmeaza:

- operatorul Autoritatii de Inregistrare primeste cererea solicitantului,
- operatorul verifica datele din cerere, cum ar fi datele personale ale solicitantului si verifica existenta dovezii posesiei cheii private,
- ca urmare a verificarii, operatorul confirma identitatea dintre datele declarate si cele cuprinse in cerere; daca cererea contine date neconforme este respinsa,
- cererea confirmata este trimisa la Autoritatea de Certificare,
- Autoritatea de Inregistrarea mai verifica si alte date care nu sunt specificate in cerere dar sunt necesare pentru emiterea certificatului.

4.2.2. La Autoritatea de Certificare (AC)

Autoritatea de Certificare verifica faptul ca cererile au fost confirmate de catre Autoritatea de Inregistrare a Furnizorului de Servicii de Certificare (FSC).

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

4.2.3. Emiterea certificatelor

Dupa primirea si procesarea unei cereri, Autoritatea de Certificare emite un certificat. Un certificat este considerat valid (in stare activa sau pregatit) in momentul acceptarii lui de catre utilizatorul final. Perioada de valabilitate a certificatelor emise depinde de tipul de certificat si de categoria utilizatorului final.

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

- cererea procesata este trimisa serverului de emitere de certificate,
- daca cererea contine solicitarea generarii unei perechi de chei, serverul cere generatorului hardware de chei acest lucru,
- se testeaza calitatea cheilor publice generate sau emise de Autoritatea de Certificare,
- daca procedurile sunt incheiate cu succes, serverul emite un certificat si insarcineaza modulul hardware de securitate cu semnarea certificatului; certificatul este stocat in baza de date a Autoritatii de Certificare,
- Autoritatea de Certificare pregateste raspunsul continand certificatul emis (daca a fost emis) si il trimite utilizatorului; certificatul emis este publicat in depozitul de la nivelul Autoritatii de Validare.

Autoritatea de Certificare AlfaTrust Certification foloseste doua metode de baza pentru anuntarea unui utilizator final despre emiterea unui certificat:

- prima metoda presupune folosirea postei sau a postei electronice si consta in trimiterea (la adresa furnizata de utilizator) a informatiilor ce permit utilizatorului sa-si ridice certificatul. Aceasta metoda este folosita si cand este necesara anuntarea tuturor utilizatorilor finali ai unei anumite Autoritati de Certificare despre emiterea unui nou certificat pentru autoritatea respectiva;
- A doua metoda consta in emiterea unui certificat si plasarea acestuia (de obicei impreuna cu o cheie privata) pe un dispozitiv criptografic si trimiterea certificatului (prin posta) la adresa utilizatorului final .

Fiecare certificat emis este publicat in depozitul AlfaTrust Certification operat la nivelul Autoritatii de Validare. Publicarea certificatului este echivalenta cu notificarea altor Entitati Partenere despre faptul ca un certificat a fost emis pentru un utilizator.

Perioadele de timp pentru emiterea certificatelor depind in primul rand de acuratetea datelor trimise in cerere si de modul de cooperare dintre AlfaTrust Certification si solicitant, precum si de modul cum s-a facut cererea – individual sau in grup, dar aceasta perioada nu va fi mai mare de 5 zile lucratoare.

In cazul in care datele necesare nu sunt puse la dispozitia Autoritatii de Inregistrare in termen, sau este necesara o completare a documentatiei, termenul de emitere a certificatului va fi prelungit.

4.2.4. Respingerea cererii de certificat

AlfaTrust Certification poate refuza in conditii bine precizate emiterea unui certificat oricarui solicitant fara a-si asuma vreo obligatie sau responsabilitate pentru posibilele daune sau pierderi pe care le poate suferi solicitantul ca urmare a acestui refuz. Autoritatea de Inregistrare va restitui solicitantului taxa de

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

certificat (daca acesta a platit-o), cu exceptia cazului in care solicitantul a mentionat date false in cererea sa.

Refuzul emiterii de certificat poate surveni in urmatoarele situatii:

- daca identificatorul solicitantului (ND) coincide cu identificatorul altui utilizator,
- daca exista suspiciune sau certitudine cu privire la falsificarea sau folosirea unor date false de catre solicitant,
- daca solicitantul, intr-o maniera de natura sa produca prejudicii, angajeaza resurse si mijloace de procesare ale AlfaTrust Certification prin trimiterea unui numar de cereri in mod clar mai mare decat nevoile pe care le are acesta,
- din alte motive decat cele de mai sus, cu conditia ca acestea sa fie argumentate.

Informatiile privind decizia refuzului de emitere de certificat si motivele acesteia sunt trimise solicitantului. Solicitantul poate cere din nou emiterea unui certificat numai dupa ce motivele care au dus la refuzul emiterii au fost inchise sau solutionate.

4.2.5. Acceptarea certificatelor

La primirea unui certificat, utilizatorul se angajeaza sa verifice continutul acestuia, in special corectitudinea datelor si complementaritatea cheii publice cu cea privata pe care o detine. Daca certificatul are nereguli sau greseli ce nu pot fi acceptate de utilizator, acesta din urma va sesiza imediat Autoritatea de Inregistrare a Furnizorului de Servicii de Certificare, in vederea revocarii certificatului.

Certificatul este considerat acceptat in ipoteza aparitiei unuia dintre urmatoarele evenimente in termen de maxim 7 zile calendaristice de la data primirii certificatului de catre utilizator:

- acceptarea explicita a certificatului emis, la momentul ridicarii certificatului de pe site-ul AlfaTrust Certification,
- primirea unui pachet inregistrat (trimis de AlfaTrust Certification) continand certificatul.

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

Fiecare certificat acceptat este publicat in depozitul Autoritatii de Validare si este accesibil publicului. Acceptarea certificatului este o decizie unilaterala a solicitantului, anterior utilizarii lui in efectuarea oricarei operatii criptografice, prin care se considera ca a acceptat termenii si conditiile specifice. In cazul trimiterii electronice a cererii, solicitantul accepta in mod automat certificatul la momentul cererii acestui certificat.

Prin acceptarea certificatului, utilizatorul final accepta regulile DPSIi si ale Politicii de Certificare si Sigilii Electronice si subscrie sa respecte prevederile contractul incheiat cu AlfaTrust Certification S.A.

4.3. Revocarea certificatelor

Revocarea unui certificat are o influenta semnificativa asupra utilizarii acestuia si asupra obligatiilor unui utilizator care detine un astfel de certificat. Imediat dupa revocarea certificatului unui utilizator final, certificatul trebuie considerat invalid (in stare de revocare). Similar, in cazul certificatului Autoritatii de

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Certificare – anularea validitatii unui certificat de acest tip semnifica retragerea drepturilor de emitere de certificate pentru proprietarul sau si revocarea tuturor certificatelor emise de aceasta.

Revocarea nu afecteaza tranzactiile facute inainte de revocare si nici obligatiile care rezulta din respectarea prezentului document.

Acest capitol specifica conditiile necesare pentru ca o Autoritate de Certificare sa aiba motive de revocare a certificatului.

Daca o cheie privata, care corespunde unei chei publice, continuta intr-un certificat revocat, ramane sub controlul utilizatorului final, dupa revocare ar trebui stocata in siguranta, pana este distrusa fizic.

4.3.1. Circumstantele revocarii certificatului

Certificatul se revoca atunci cand:

- informatia continuta de certificat s-a schimbat,
- o cheie privata, asociata unei chei publice, continuta in certificat sau pe dispozitivul de stocare, a fost compromisa sau exista un motiv serios pentru a suspecta ca a putut fi compromisa,
- partile decid sa inceteze contractul incheiat de acestea; in acest caz, revocarea este strict legata de anularea inregistrarii utilizatorului final la Autoritatea de Inregistrare a FSC-ului; daca utilizatorul insusi nu cere revocarea, Autoritatea de Certificare sau un reprezentant al institutiei la care este angajat utilizatorul, au dreptul sa o faca,
- Abonatul, detinatorul unei chei publice, cere revocarea,
- poate fi revocat de emitent (Furnizorul de Servicii de Certificare), daca un utilizator nu respecta Politica de Certificare si Sigilii Electronice, DPSI sau contractul, ori alte documente emise de Furnizorul de Servicii de Certificare,
- Furnizorul de Servicii de Certificare isi inceteaza activitatea; in acest caz toate certificatele emise de aceasta Autoritate de Certificare, inainte de expirarea perioadei declarate pentru oprirea serviciilor, trebuie revocate impreuna cu certificatul Autoritatii de Certificare,
- Abonatul intarzie sau nu plateste contravaloarea serviciile prestate de catre Furnizorul de Servicii de Certificare,
- cheia privata sau securitatea unei Autoritati de Certificare a fost compromisa intr-un mod in care pune in pericol credibilitatea certificatelor,
- Abonatul, angajat al unei organizatii, nu a returnat dispozitivul criptografic folosit pentru stocarea certificatului si a cheii private corespunzatoare, la incheierea contractului de munca,
- in alte cazuri in care utilizatorul final nu se conformeaza regulilor acestei DPSI, Politicii de Certificare si Sigilii Electronice, sau contractului.

Sintagma “cheie privata compromisa” este folosita in unul din urmatoarele sensuri:

- accesul neautorizat la cheia privata sau un motiv intemeiat pe baza caruia sa se suspecteze ca acest acest acces s-a petrecut,
- pierderea cheii private sau aparitia unui motiv de a suspecta o astfel de pierdere,
- furtul cheii private sau aparitia unui motiv de a suspecta un astfel de furt,
- stergerea accidentala a cheii private.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

4.3.2. Cine poate solicita revocarea

Urmatoarele entitati pot trimite cereri de revocare a certificatului unui utilizator final:

- utilizatorul insusi, cu conditia sa fie proprietarul certificatului,
- un reprezentant autorizat al Furnizorul de Servicii de Certificare,
- un reprezentant al utilizatorul final, de exemplu angajatorul sau; utilizatorul trebuie imediat informat despre acest lucru,
- Autoritatea de Inregistrare poate cere revocarea in numele unui utilizator, sau in nume propriu, daca are informatii care justifica revocarea certificatului.

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

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

Fiecare cerere va fi trimisa trimisa:

- direct Autoritatii de Inregistrare sub forma electronica, cu sau fara confirmarea Autoritatii de Inregistrare,
- indirect (prin intermediul unui tert) la sediul Furnizorul de Servicii de Certificare, sub forma ne-electronica (document pe hartie, fax, telefon etc.).

4.3.3. Procedura de revocare

Revocarea certificatului se poate face in urmatoarele moduri:

i. prin trimiterea unei cereri de revocare in format electronic catre o Autoritate de Inregistrare; o astfel de revocare poate fi initiata numai la cererea utilizatorul final; aceasta metoda se aplica in situatiile in care:
    a. Abonatul a pierdut cheia sa privata sau parola ei, sau cheia privata a fost furata sau
    b. cererea de revocare a fost trimisa de reprezentantul utilizatorul final, cu conditia de a exista suficiente motive pentru a cere o astfel de revocare;

ii. prin trimiterea unei cereri ne-electronice autentificate (document pe hartie, fax, telefon etc.) catre AlfaTrust Certification ; autentificarea unui document pe hartie (inclusiv faxul) poate fi efectuata la Autoritatea de Inregistrare, de exemplu cu o stampila si o semnatura de mana a unei persoane recunoscute de AlfaTrust Certification; o cerere facuta prin telefon este indeplinita numai dupa ce se trimit si documentele de autentificare a solicitantului; dupa verificarea cu succes a cererii, Autoritatea de Inregistrare pregateste confirmarea electronica a cererii de revocare si o inainteaza Autoritatii de Certificare.

Informatiile despre certificatele revocate sunt plasate in Lista de Certificate Revocate, la nivelul Autoritatii de Validare AlfaTrust Certification. Autoritatea de Inregistrare notifica entitatea care cere revocarea certificatului despre aceasta revocare, sau despre decizia de a anula cererea, impreuna cu motivele anularii.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Procedura de revocare a unui certificat se desfasoara astfel:

- Autoritatea de Inregistrare, ca urmare a primirii unei cereri de revocare certificat, o verifica; daca cererea este facuta electronic, Autoritatea de Inregistrare verifica corectitudinea certificatului de revocat si corectitudinea certificatului atasat cererii; cererea facuta pe hartie necesita autorizarea solicitantului; o astfel de confirmare poate fi obtinuta prin telefon, fax sau prin prezentarea in persoana a utilizatorul final la un reprezentant autorizat al Autoritatii de Inregistrare (sau invers);
- daca cererea este verificata cu succes, Autoritatea de Certificare plaseaza informatiile despre revocarea certificatului in Lista certificatelor Revocate (CRL), impreuna cu informatii privind motivele de revocare;
- Autoritatea de Inregistrare notifica, electronic sau prin posta, entitatea care cere revocarea despre revocare sau decizia de anulare a cererii impreuna cu motivele anularii.
- in plus, daca partea care cere revocarea nu este utilizatorul final, Autoritatea de Inregistrare va notifica utilizatorul in privinta revocarii certificatului, sau initierii procesului de revocare.

Daca un certificat, sau o cheie privata corespunzatoare unui certificat de revocat au fost stocate pe un dispozitiv criptografic, ca urmare a revocarii certificatului, dispozitivul criptografic trebuie distrus fizic sau sters in coditii de maxima securitate. Aceasta operatie se indeplineste de catre posesorul dispozitivului criptografic – o persoana fizica sau juridica (un reprezentant al unei astfel de entitati). Detinatorul dispozitivului criptografic trebuie sa-l pastreze astfel incat sa previna furtul sau utilizarea neautorizata a sa pana la distrugerea fizica sau la stergerea cheii private.

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

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

In momentul revocarii certificatului, operatorii Autoritatii de Inregistrare si utilizatorii implicati sunt informati automat despre aceasta revocare. Informatii despre starea curenta a certificatului sunt disponibile prin serviciul de verificare a starii certificatelor imediat dupa perioada de gratie declarata. Acest serviciu poate fi cerut, de exemplu, de catre o Entitate Partenera, care verifica validitatea unei semnaturi electronice aplicate unui document primit de la utilizatorul final.

4.3.4. Frecventa de emitere a CRL-urilor

Fiecare Autoritate de Certificare care face parte din domeniul AlfaTrust Certification emite diferite Liste de Certificate Revocate. Un nou CRL este publicat in depozit dupa fiecare revocare de certificat, intr-un interval de maxim o zi. Daca motivul revocarii este compromiterea cheii, noul CRL este emis imediat dupa procesarea cererii de revocare. Perioada de valabilitate a CRL-ului este de 24 de ore si se actualizeaza zilnic.

Lista de certificate Revocate (CRL) pentru autoritatea AlfaTrust Certification ROOT CA (SHA sau SHA256) este emisa cel putin in fiecare an cu conditia sa nu existe nici o revocare de certificat a uneia dintre autoritatile direct subordonate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

In cazul revocarii certificatului unei autoritati afiliate la AlfaTrust Certification, acest certificat este imediat publicat in Lista de certificate Revocate.

4.3.5. Verificarea listei de certificate revocate (CRL)

O Entitate Partenera, ca urmare a primirii unui document electronic semnat de un utilizator final, este obligata sa verifice daca certificatul cheii publice corespunzatoarea cheii private a utilizatorului, folosita pentru crearea de semnaturi electronice, nu este plasat in Lista de certificate Revocate. Entitatea Partenera este obligata sa foloseasca CRL-ul curent.

Verificarea starii unui certificat se poate baza in exclusivitate pe consultarea CRL-ului numai in cazurile in care frecventa perioadelor de emitere a CRL-ului, declarata de AlfaTrust Certification, nu poate aduce daune serioase sau pierderi pentru Entitatea Partenera. In alte cazuri, o Entitate Partenera este obligata sa foloseasca serviciul de verificare on-line a starii certificatelor (OCSP).

Daca un certificat de verificat este plasat intr-un CRL, entitatea partenera este obligata sa respinga documentul asociat acestui certificat, daca motivul revocarii este unul dintre urmatoarele:

i. **unspecified, certificateHold** – necunoscut,
ii. **keyCompromise** – compromiterea securitatii cheii private,
iii. **cACompromise** – compromiterea securitatii Autoritatii de Certificare,
iv. **cessationOfOperation** – incetarea serviciilor asociate cheii private,

Decizia finala asupra credibilitatii certificatului se va lua de catre Entitatea Partenera daca un certificat a fost revocat din urmatoarele motive:

v. **affiliationChanged** – modificarea datelor,
vi. **superseded** – modificarea cheii.

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

AlfaTrust Certification ofera serviciul de verificare in timp real a starii unui certificat. Acest serviciu se realizeaza pe baza protocolului OCSP, descris in RFC 2560. Folosind OCSP este posibil sa se obtina date mai exacte (in comparatie cu folosirea exclusiva a CRL-ului) despre starea unui certificat.

OCSP functioneaza pe baza modelului cerere-raspuns. Ca raspuns la o cerere, serverul OCSP, ofera urmatoarele informatii despre starea certificatului:

* ***good*** – semnificand un raspuns pozitiv pentru cerere, care trebuie interpretat ca fiind confirmarea validitatii certificatului,
* ***revoked*** – insemnand ca certificatul a fost revocat,
* ***unknown*** – semnificand ca certificatul nu a fost emis de nici una dintre Autoritatile de Certificare afiliate.

Serviciul OCSP este disponibil oricarui utilizator final si Entitate Partenera care a semnat contractul cu AlfaTrust Certification in legatura cu oferirea acestor servicii.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

Starea certificatului este intotdeauna oferita in timp real (imediat dupa revocarea certificatului) pe baza informatiilor din baza de date a AlfaTrust Certification si contine informatii mai noi decat cele din CRL-ul publicat.

O Entitate Partenera nu este obligata sa verifice on-line starea certificatelor pe baza serviciilor si mecanismelor de mai sus. Totusi, este recomandata folosirea serviciului OCSP atunci cand riscul falsificarii documentelor electronice prin folosirea semnaturii electronice este mare sau daca acest lucru este cerut de alte reglementari care vizeaza astfel de situatii.

4.3.7. Revocarea certificatului Autoritatii de Certificare (AC)

Certificatul apartinand unei Autoritati de Certificare poate fi revocat de catre autoritatea emitenta. O astfel de revocare poate sa apara in urmatoarele situatii:

- Autoritatea de Certificare are motive sa creada ca datele din certificatul autoritatii respective nu corespund realitatii,
- cheia privata a Autoritatii de Certificare sau sistemul sau informatic au fost compromise astfel incat afecteaza credibilitatea certificatelor emise de aceasta autoritate,
- Autoritatea de Certificare a incalcat obligatiile materiale care reies din aceasta DPSI, Politica de Certificare si Sigilii Electronice sau contract.

4.4. Schimbarea cheii unei Autoritati de Certificare (AC)

Procedurile de schimbare a cheii (*key changeover*) se aplica cheilor Autoritatilor de Certificare afiliate la AlfaTrust Certification si descriu modul in care se face schimbarea cheilor certificatelor autoritatilor, folosite pentru semnarea certificatelor utilizatorilor sau CRL-urilor. Procedura de schimbare a cheii se bazeaza pe emiterea de catre Autoritatea de Certificare a unui certificat special, ce permite unui utilizator care detine vechiul certificat al autoritatii sa-l obtina pe cel nou iar noilor utilizatori care au deja noul certificat al autoritatii sa-l obtina pe cel vechi pentru verificarea datelor curente. Fiecare schimbare de cheie a Autoritatii de Certificare este anuntata in avans prin intermediul paginilor de web ale AlfaTrust Certification si difuzata prin posta electronica catre fiecare utilizator al Autoritatii de Certificare a carei chei urmeaza a fi schimbate. In plus, in cazul schimbarii cheii AlfaTrust Certification ROOT CA, informatiile despre acest eveniment vor fi publicate prin intermediul mass-media cu o luna inainte de momentului expirarii perioadei de valabilitatea a cheii private. Frecventa schimbarii cheilor unei Autoritati de Certificare afiliata la AlfaTrust Certification este data de perioada de valabilitate a certificatului autoritatii.

Din momentul schimbarii cheii, Autoritatea de Certificare foloseste numai noua cheie privata pentru semnarea certificatelor emise si a CRL-urilor.

4.5. Incetarea activitatii unui Furnizor de Servicii de Certificare (FSC) sau transferarea serviciilor

Obligatiile prezentate mai jos sunt stabilite pentru a minimiza efectele negative asupra utilizatorilor finali si Entitatilor Partenere, ce pot apare ca urmare a deciziei unui Furnizor de Servicii de Certificare de a-si

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

inceta activitatea si se refera la obligatiile de a notifica in prealabil toti utilizatorii ca isi inceteaza activitatea si transferarea responsabilitatilor (servicii oferite utilizatorilor finali, baza de date, etc.), conform reglementarilor in vigoare, unui alt Furnizor de Servicii de Certificare.

4.5.1. Transferul responsabilitatii

Inainte ca un Furnizor de Servicii de Certificare sa-si inceteze activitatea, este obligat sa:

- anunte Autoritatea de Certificare care a emis certificatul sau despre intentia de a-si inceta activitatea ca Furnizor de Solutii de Certificare; notificarea trebuie facuta cu 90 de zile inainte de data stabilita pentru incetarea efectiva a activitatii,
- sa anunte (cu cel putin 30 de zile inainte) utilizatorii sai care au certificate active (neexpirate si nerevocate) emise de autoritatea respectiva despre decizia de a-si inceta activitatea,
- sa revoce toate certificatele care raman active (neexpirate si nerevocate) in momentul declarat al incetarii activitatii, indiferent daca utilizatorul a trimis sau nu o cerere in acest sens,
- sa anunte toti utilizatorii Furnizorului de Solutii de Certificare despre incetarea activitatii,
- sa depuna toate eforturile pentru a minimiza efectele negative asupra intereselor utilizatorilor si persoanelor juridice angajate in procese de verificare a semnaturilor electronice folosind certificate digitale emise de FSC-ul care isi incheie activitatea,
- sa propuna incheierea unui contract (de exemplu cu un alt Furnizor de Solutii de Certificare) prin care sa se garanteze protectia datelor,
- sa plateasca compensatii (care sa nu depaseasca taxele de emitere si depozitare a certificatelor) utilizatorilot al caror certificat neexpirat si nerevocat va fi revocat inainte de data expirarii.

4.5.2. Emiterea certificatelor de catre succesor

Pentru a asigura continuitatea serviciilor de emitere de certificate pentru utilizatorii finali, Furnizorul de Servicii de Certificare care isi inceteaza activitatea poate semna un contract cu alt FSC ce ofera servicii similare, pentru a emite certificate care sa inlocuiasca certificatele ramase in uz, emise de FSC-ul care isi incheie activitatea.

Prin emiterea unui certificat care sa-l inlocuiasca pe cel vechi, succesorul Furnizorului de Servicii de Certificare care isi inceteaza activitatea preia drepturile si obligatiile acestei autoritati in ceea ce priveste managementul certificatelor care raman in uz.

5. Masurile de securitate InfoSEC

Prin definitie, termenul InfoSEC reprezinta protectia surselor generatoare de informatii. In sens mai larg, prin InfoSEC se intelege ansamblul masurilor si structurilor de protectie a informatiilor care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice si de comunicatii si al altor sisteme electronice, impotriva amenintarilor si a oricaror actiuni care pot aduce atingere confidentialitatii, integritatii, disponibilitatii, autenticitatii si non-repudierii informatiilor, precum si afectarea functionarii sistemelor informatice, indiferent daca acestea apar accidental sau intentionat.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Masurile de securitate (controalele) InfoSEC acopera securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografica, precum si depistarea si prevenirea amenintarilor la care sunt expuse informatiile si sistemele.

In sensul celor de mai sus definim si:

* **securitatea comunicatiilor (ComSEC)** = aplicarea masurilor de securitate in retelele de comunicatii, cu scopul de a proteja mesajele dintr-un sistem de comunicatii, care ar putea fi interceptate, studiate, analizate si, prin reconstituire, pot conduce la dezvaluiri de informatii sensibile. ComSEC reprezinta ansamblul de:
  - masuri de securitate a transmisiilor (TranSEC);
  - masuri de securitate impotriva radiatiilor (EmSEC sau TEMPEST);
  - masuri de securitate criptografica;
  - masuri de securitate fizica, procedurala, de personal si a documentelor;
* **securitatea calculatoarelor si a retelelor de calculatoare (CompuSEC)** = aplicarea la nivelul fiecarui calculator si/sau retea de calculatoare a facilitatilor de securitate hardware, software si firmware, pentru a preveni divulgarea, manevrarea, modificarea sau stergerea neautorizata a informatiilor sensibile ori invalidarea neautorizata a unor functii;

5.1. Controale ComSEC

5.1.1. Controale de securitate criptografica (cryptosecurity)

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

5.1.1.1. Generarea si folosirea perechii de chei

Procedurile de management a cheii se refera la pastrarea si folosirea in siguranta de catre proprietar a cheilor sale. O atentie deosebita se acorda generarii si protectiei cheii private a AlfaTrust Certification ROOT CA, care influenteaza functionarea in siguranta a intregului sistem de certificare a cheilor publice.

Autoritatea de Certificare AlfaTrust Certification ROOT CA detine cel putin un certificat autosemnat. Cheia privata corespunzatoare cheii publice continuta de certificatul autosemnat este folosita exclusiv in scopul semnarii cheilor publice ale Autoritatilor de Certificare direct subordonate (de pe nivelul 1 de certificare), prin semnarea certificatelor operationale si a Listei de certificate Revocate, necesare pentru functionarea autoritatilor respective.

Perechile de chei detinute de fiecare Autoritate de Certificare de pe nivelul 1 de certificare (SubCA-urile) permit semnarea de certificate si CRL-uri - o cheie publica asociata cu o cheie privata autentificata cu un certificat autosemnat (in cazul AlfaTrust Certification ROOT CA) sau certificat (in cazul SubCA-urilor).

Semnatura electronica este creata prin folosirea algoritmului RSA in combinatie cu rezumatul criptografic SHA-1 sau SHA-256.**Generarea perechilor de chei**

Cheile Autoritatilor de Certificare de pe nivelul 1 de certificare (SubCA-urile), precum si ale altor autoritati subordonate acestora sunt generate in cadrul locatiei AlfaTrust Certification, in prezenta unui grup de

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

persoane de incredere (administratorul de securitate si administratorul Autoritatii de Certificare sunt membri ai acestui grup).

Perechile de chei pentru Autoritatile de Certificare care functioneaza in cadrul AlfaTrust Certification sunt generate la anumite statii de lucru autentificate si conectate la module hardware de securitate (HSM), conforme cu cerintele FIPS 140-2 Nivel 3. Ele sunt mentinute in permanenta criptate pe aceste dispozitive.

Procesul de generare de perechi de chei pentru Autoritatile de Certificare este similar cu procedura acceptata de generare a cheilor in cadrul AlfaTrust Certification. Actiunile intreprinse in momentul generarii perechii de chei sunt inregistrate, datate si semnate de fiecare persoana prezenta in timpul generarii. Inregistrarile sunt pastrate din motive de audit sau pentru verificarile obisnuite ale sistemului.

Operatorii Autoritatii de Inregistrare detin numai chei pentru autentificarea tuturor actiunilor lor. Aceste chei sunt generate de operator (in prezenta administratorilor de secrete) prin intermediul unei aplicatii software autentificata, furnizata de Autoritatea de Certificare si conectata la un modulul hardware de securitate conform cu cerintele FIPS 140-2 Nivel 2.

In general, fiecare utilizator final isi genereaza singur perechea de chei. Pentru aceasta se va folosi de aplicatia disponibila pe site-ul web al AlfaTrust Certification, in momentul crearii cererii. Aplicatia permite crearea cheilor atat pe dispozitive securizate (tokenuri, smart carduri), cat si in format “PKCS#12” criptat. Generarea poate fi, de asemenea, facuta de catre o Autoritate de Certificare.

AlfaTrust Certification poate, la cererea utilizatorului sau la cererea operatorului Autoritatii de Inregistrare, sa genereze o pereche de chei si sa o trimita in siguranta utilizatorul final. In astfel de cazuri sunt folosite aplicatii si dispozitive criptografice conforme cu FIPS 140-2 Nivel 2.

Procedurile de generare a cheilor initiale ale Autoritatii de Certificare Primara

Procedurile de generare a cheii initiale a AlfaTrust Certification ROOT CA sunt folosite numai la initierea sistemului AlfaTrust Certification sau in cazul suspectarii faptului ca cheia privata a Autoritatii de Certificare Primara a fost compromisa. Procedura include:

- generarea in siguranta a perechii principale de chei pentru semnarea de certificate si CRL-uri si distribuirea cheii private,
- emiterea unui certificat de cheie publica autosemnat.

Dupa generarea perechii de chei pentru semnarea de certificate si CRL-uri, activarea cheii private in modulul hardware de securitate, cheile pot fi folosite in operatiile criptografice pana la expirarea perioadei de validitate sau pana cand au fost compromise.

Procedura de schimbare a cheii certificatului pentru Autoritatea de Certificare Primara

Cheile criptografice ale Autoritatii de Certificare Primara (AlfaTrust Certification ROOT CA) au o perioada de viata limitata; daca aceasta perioada a expirat, cheile trebuie actualizate.

Actualizarea perechii de chei folosite pentru semnarea de certificate si CRL-uri se face folosind o procedura specifica. Aceasta se bazeaza pe emiterea de certificate speciale de catre AlfaTrust Certification ROOT CA.

Certificatele dau posibilitatea utilizatorilor care au instalat deja un certificat expirat al AlfaTrust Certification ROOT CA sa treaca in siguranta la utilizarea noului certificat; noii utilizatori care poseda deja

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

noul certificat pot sa obtina in siguranta certificatul expirat, care poate fi necesar la verificarea datelor semnate in trecut.

Pentru a obtine efectul descris mai sus, AlfaTrust Certification ROOT CA aplica o procedura prin intermediul careia generarea unei noi perechi de chei va permite autentificarea noii chei publice prin folosirea cheii private vechi si invers (o cheie publica veche este autentificata cu o cheie privata noua). Aceasta inseamna ca, drept rezultat al actualizarii certificatului Autoritatii de Certificare, AlfaTrust Certification ROOT CA, in afara de certificatul nou, mai sunt create inca doua certificate.

Dupa actualizarea cheii, sunt create patru certificate pentru semnarea de certificate si CRL-uri:

- certificatul vechi ***OldWithOld*** (cheia publica veche este semnata cu cheia privata veche),
- certificatul nou ***NewWithNew*** (cheia publica noua este semnata cu cheia privata noua),
- certificatul ***OldWithNew*** (cheia publica veche este semnata cu cheia privata noua) si
- certificatul ***NewWithOld*** (cheia publica noua este semnata cu cheia privata veche).

Procedura de actualizare a perechii de chei pentru AlfaTrust Certification ROOT CA, folosita pentru semnarea de certificate si CRL-uri, se desfasoara astfel:

- generarea unei perechi de chei noi,
- crearea unui certificat continand cheia publica noua a AlfaTrust Certification ROOT CA, semnat cu cheia privata vechea (certificatul NewWithOld),
- dezactivarea cheii private vechi si activarea celei noi in modulul hardware de securitate – este incarcata cheia privata noua pentru semnarea de certificate si CRL-uri,
- crearea unui certificat continand cheia publica veche a AlfaTrust Certification ROOT CA, semnat cu cheia privata noua (certificatul OldWithNew),
- crearea unui certificat continand cheia publica noua a AlfaTrust Certification ROOT CA, semnat cu cheia privata noua (certificatul NewWithNew),
- publicarea in depozit a noilor certificate, difuzarea de informatii despre noile certificate disponibile si, optional, publicarea rezumatului criptografic al noii chei publice in ziare.

Dupa generarea si activarea cheii private noi (acest lucru se poate face in orice moment, in timpul perioadei de validitate a vechiului certificat), autoritatea AlfaTrust Certification ROOT CA semneaza noile certificate folosind exclusiv noua cheie privata.

Vechea cheie publica (vechiul certificat) este disponibila publicului pana cand toti utilizatorii obtin noul certificat (noua cheie publica) a AlfaTrust Certification ROOT CA (acesta trebuie obtinuta inaintea datei de expirare a vechiului certificat).

Inceputul si expirarea perioadei de validitate a certificatului *OldWithNew* este aceeasi cu data de inceput si de expirare a certificatului vechi.

Perioada de validitate a certificatului *NewWithOld* incepe din momentul generarii noii perechi de chei si expira in momentul in care toti utilizatorii finali vor obtine noile certificate (certificatul noii chei publice) ale AlfaTrust Certification ROOT CA. Momentul expirarii nu este mai mare decat cel al expirarii vechiului certificat.

Perioada de validitate a certificatului *NewWithNew* incepe din momentul generarii noii perechi de chei si expira la cel putin 180 de zile dupa data urmatoarei generari de perechi de chei. Acest lucru inseamna ca Autoritatea de Certificare AlfaTrust Certification ROOT CA inceteaza a mai folosi cheia privata pentru

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

semnarea de certificate si CRL-uri cu cel putin 180 de zile inainte de data expirarii certificatului corespunzator acestei chei private.

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

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

- generarea in siguranta a perechii principale de chei pentru semnarea de certificate si CRL-uri si distribuirea cheii private,
- emiterea unui certificat de cheie publica semnat de AlfaTrust Certification ROOT CA.

Dupa generarea perechii de chei pentru semnarea de certificate si CRL-uri si activarea cheii private in modulul hardware de securitate, cheile pot fi folosite in operatiile criptografice pana la expirarea perioadei de validitate sau pana la o eventuala compromitere.

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

Procedura de schimbare (actualizare) a cheilor Autoritatilor de Certificare pentru AlfaTrust Certification SubCA-uri se desfasoara in mod similar cu cea pentru AlfaTrust Certification ROOT CA cu exceptia unui singur pas: certificatul *NewWithNew* este emis de catre autoritatea superioara.

5.1.1.1.2. Distribuirea cheii private

Daca perechea de chei a utilizatorului este generata de catre o Autoritate de Certificare, cheile se distribuie utilizatorului astfel:

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

AlfaTrust Certification garanteaza ca dupa generarea perechii de chei la cererea unui utilizator, cheile nu vor fi folosite pentru crearea de semnaturi electronice si ca Autoritatea de Certificare nu va crea conditii pentru crearea de semnaturi de catre nici o entitate neautorizata, cu exceptia proprietarului cheii private.

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

Abonatii trimit cheia lor publica generata sub forma de cerere electronica, al carui format trebuie sa respecte standardul PKCS#10 (CRS).

Cererile trimise unei Autoritati de Inregistrare pot necesita, in anumite cazuri, o confirmare emisa de Autoritatea de Inregistrare.

Trimiterea cheii publice nu este necesara atunci cand perechea de chei este generata, la cererea utilizatorului sau la cererea operatorului Autoritatii de Inregistrare, de catre Autoritatea de Certificare, care emite simultan un certificat pentru perechea de chei generata.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

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

Cheile publice ale unei Autoritati de Certificare care emite certificate catre utilizatori sunt distribuite in exclusivitate sub forma de certificate conform recomandarilor ITU-T X.509 v.3. In cazul Autoritatii de Certificare AlfaTrust Certification ROOT CA, certificatele sunt autosemnate.

Autoritatile de Certificare AlfaTrust Certification distribuie certificatele proprii in doua moduri diferite:

- prin plasarea in depozitul public al AlfaTrust Certification; obtinerea certificatelor necesita vizitarea paginii web disponibila la http://www.AlfaSign.ro/,
- distribuirea impreuna cu aplicatiile software (browsere Web, clienti de email etc.), care permit folosirea serviciilor oferite de AlfaTrust Certification .

In cazul schimbarii (actualizarii) cheii Autoritatii de Certificare AlfaTrust Certification-ROOT CA, depozitul va contine toate certificatele autosemnate sau certificatele emise

5.1.1.1.5. Dimensiunea cheilor

Dimensiunea cheilor folosite de Autoritatile de Certificare, operatorii Autoritatii de Inregistrare si utilizatorii finali sunt :

- AlfaTrust Certification ROOT CA = 2048 biti;
- AlfaTrust Certification SubCA-uri = 2048 biti;
- Operatorii Autoritatii de Inregistrare = 1024 biti sau 2048 biti;
- Persoane (fizice sau juridice) si dispozitivele hardware ale acestora = 1024 biti sau 2048 biti.

5.1.1.1.6. Parametrii de generare a cheilor publice si verificarea calitatii parametrilor

Cine genereaza o cheie este responsabil de verificarea calitatii parametrilor cheii generate.

Acesta trebuie sa verifice:

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

5.1.1.1.7. Generarea cheilor hardware si/sau software

Metodele permise pentru generarea de chei depind de politica de certificare aplicata si sunt:

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

In cazul Autoritatilor de Certificare, cheile sunt generate prin intermediul modulelor hardware de securitate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Cheile operatorilor Autoritatii de Inregistrare sunt generate utilizand module hardware de securitate (HSM). In cazul generarii cheii de catre un utilizator, Autoritatea de Certificare accepta atat metode de generare hardware cat si software.

5.1.1.1.8. Folosirea cheilor

Scopurile in care pot fi folosite cheile sunt date de campul *KeyUsage* din cadrul extensiilor standard ale certificatelor X.509 v3. Acest camp trebuie verificat in mod obligatoriu de aplicatia utilizatorul final care face managementul certificatelor.

Folosirea bitilor din campul *KeyUsage* trebuie sa respecte urmatoarele reguli:

a. ***digitalSIGNature***: certificat pentru verificarea de semnaturi electronice,
b. ***nonRepudiation***: certificat pentru furnizarea de servicii de non-repudiere catre persoane fizice, cat si pentru alte scopuri decat cele descrise la punctele f) si g). Bitul de non-repudiere poate fi setat numai intr-un certificat de cheie publica cu care se intentioneaza verificarea semnaturilor electronice si nu trebuie combinat cu cele descrise la punctele c) - e) si in legatura cu asigurarea confidentialitatii,
c. ***keyEncipherment***: folosit pentru a cripta cheile pentru algoritmi simetrici, oferind confidentialitatea datelor,
d. ***dataEncipherment***: folosite pentru criptarea datelor utilizatorului, altele decat cele de la punctele c) si e),
e. ***keyAgreement***: folosit in protocoale de schimb de chei,

f. ***cRLSign***: cheia publica este folosita pentru verificarea semnaturilor electronice de pe listele de certificate revocate si suspendate emise de entitatile care ofera servicii de certificare,
g. ***encipherOnly***: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica criptarea datelor in procesul de schimb de chei,
h. ***decipherOnly***: poate fi folosit exclusiv cu bitul de *keyAgreement* pentru a indica decriptarea datelor in procesul de schimb de chei.

5.1.1.2. Protectia cheii private

Fiecare utilizator, operator al Furnizorului de Servicii de Certificare si Autoritate de Certificare genereaza si stocheaza cheia sa privata folosind un sistem sigur care previne pierderea, dezvaluirea, modificarea sau accesul neautorizat la aceasta cheie. Daca o Autoritate de Certificare genereaza o pereche de chei la cererea utilizatorul final, trebuie sa o livreze acestuia in siguranta si sa impuna utilizatorului protejarea cheii sale private.

5.1.1.2.1. Standarde pentru modulele criptografice

Modulele hardware de securitate (HSM) folosite de Autoritatile de Certificare respecta cerintele standardului FIPS 140-2. In cazul utilizatorilor care folosesc mecanisme hardware de protectie a cheii, se recomanda de asemenea respectarea cerintelor FIPS 140-2 sau Common Criteria.

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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Cheile private (ca si cheile publice) pot fi in una dintre urmatoarele stari (in conformitate cu standardul ISO/IEC 11770-1):

- ***in asteptare pentru activare (pregatita)*** – cheia a fost deja generata, dar nu este utilizabila (data curenta nu este inca aceeasi cu data inceperii perioadei de validitate a certificatului),
- ***activa*** – cheia poate fi folosita in operatiile criptografice (de exemplu pentru crearea de semnaturii electronice), data curenta este in cadrul perioadei de validitate a certificatului, cheia nu a fost revocata,
- ***inactiva*** – cheia aflata in aceasta stare poate fi folosita numai pentru verificarea de semnaturii electronice sau pentru operatii de decriptare (utilizatorului nu-i este permisa folosirea cheii private pentru crearea de semnaturi electronice – validitatea cheii a expirat; in cazul unei chei publice, utilizatorului nu ii este permisa criptarea informatiei); data curenta este in afara perioadei de validitate a certificatului.

5.1.1.2.2. Controlul dual al accesului cheii private

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

Controlul dual al accesului se realizeaza prin distribuirea de secrete operatorilor autorizati. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN si transferate in mod autentificat detinatorilor acestora.

Pentru operatiuni de tipul: initierea modulului criptografic hardware (HSM), transferul cheilor private ale Autoritatilor de Certificare, se implementeaza scheme prag de acces (de forma k din n) prin distribuire de secrete partajate. Numarul acceptat de secrete partajate si numarul necesar de secrete care permit restaurarea cheii private sunt:

- *numarul de secrete partajate:* ***2***
- *numarul total de secrete distribuite:* ***3***

Pentru asigurarea serviciului de recuperare a cheilor private ale utilizatorilor finali se utilizeaza de asemenea scheme prag de acces. Numarul acceptat de secrete partajate este **2** si numarul necesar de secrete care permit restaurarea cheii private este **3**.

Procedura de transfer a secretului partajat implica prezenta detinatorului de secret pe timpul procesului de generare a cheii si a distribuirii sale, acceptarea secretului dat si a responsabilitatilor care reies din pastrarea sa.

5.1.1.2.2.1. Acceptarea pastrarii secretului de catre detinatori

Fiecare detinator de secret partajat, inainte de a primi partea sa de secret, trebuie sa asiste personal la impartirea secretului, sa verifice corectitudinea secretului creat si distribuirea sa.

Fiecare parte a secretului partajat trebuie transferata detinatorului pe un card criptografic protejat de un cod PIN, ales de detinator si stiut numai de el. Primirea secretului partajat si crearea sa sunt confirmate printr-o semnatura de mana pe un formular, a carui copie este pastrata in arhivele Autoritatii de Certificare si de catre detinatorul de secret.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.1.1.2.2.2. Protectia secretului partajat

Detinatorii secretului partajat trebuie sa protejeze partea lor impotriva dezvaluirii. Detinatorul declara ca:

- nu va dezvalui, copia sau imparti secretul cu nimeni si ca nu va folosi partea sa din secret intr-un mod neautorizat,
- nu va dezvalui (direct sau indirect) ca este detinatorul secretului

5.1.1.2.2.3. Disponibilitatea si stergerea (transferul) secretului partajat

Detinatorul secretului partajat trebuie sa permita accesul la partea sa din secret persoanelor juridice autorizate (printr-un formular corespunzator semnat de catre detinator inaintea oferirii partii sale din secret), numai dupa autorizarea transmiterii secretului. Aceasta situatie trebuie inregistrata in mod corespunzator in log-urile de securitate.

In cazul dezastrelor naturale, detinatorul secretului trebuie sa se prezinte la locul de recuperare in caz de urgenta al AlfaTrust Certification, in conformitate cu instructiunile primite. Secretul partajat trebuie livrat personal de catre detinator la locul recuperarii in caz de urgenta, intr-un mod care sa permita folosirea lui pentru restaurarea conditiilor normale de activitate ale AlfaTrust Certification.

5.1.1.2.2.4. Responsabilitatile detinatorului de secret partajat

Detinatorul de secret partajat trebuie sa-si indeplineasca indatoririle si obligatiile conform cerintelor acestei DPSI, in mod responsabil in orice situatie posibila. Un detinator de secret partajat trebuie sa anunte emitentul secretului in cazul furtului, pierderii, dezvaluirii neautorizate sau compromiterii securitatii secretului, imediat dupa incident. Un detinator de secret partajat nu este responsabil pentru neindeplinirea indatoririlor/obligatiilor sale din cauza unor motive ce sunt imposibil de controlat de catre acesta, dar este responsabil pentru dezvaluirea inoportuna a secretului sau pentru neglijarea obligatiilor de a notifica emitentul secretului despre dezvaluirea inoportuna sau violarea securitatii secretului ca urmare a greselilor, neglijentei sau iresponsabilitatii detinatorului.

5.1.1.2.3. Back-up-ul cheilor private

Autoritatile de Certificare care opereaza in cadrul AlfaTrust Certification creeaza o copie de siguranta a cheii lor private. Copiile sunt folosite in cazul punerii in aplicare a procedurilor standard, sau de urgenta (de exemplu, dupa dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secrete partajate.

AlfaTrust Certification nu pastreaza copii ale cheilor private ale operatorilor Autoritatii de Certificare. Copiile cheilor private ale utilizatorilor sunt create numai la cererea utilizatorul final si in conformitate cu DPSI si politicile de certificare.

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

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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.1.1.2.4. Arhivarea cheii private

Cheile private ale Autoritatii de Certificare folosite pentru crearea de semnaturi electronice nu sunt arhivate – sunt distruse imediat dupa terminarea operatiilor criptografice ce necesita aceste chei sau la expirarea/revocarea certificatului cheii publice asociate.

5.1.1.2.5. Introducerea cheii private in modulul criptografic

Operatiunea de introducere a unei chei private intr-un modul criptografic se aplica in urmatoarele cazuri:

- cand cheile sunt generate in afara modulului criptografic; aceasta situatie apare, de exemplu, in cazul generarii cheii de catre o Autoritate de Certificare la cererea utilizatorului, la introducerea lor intr-un dispozitiv criptografic, inainte de trimiterea suportului de stocare catre utilizatorul final. O operatie similara de introducere a cheii intr-un modul criptografic poate fi indeplinita de un utilizator cand cheile sunt livrate sub forma criptata si necesita stocare locala pe un dispozitiv criptografic,
- in cazul crearii copiilor de siguranta ale cheilor private stocate intr-un modul criptografic, poate fi necesara, ocazional (ex. in cazul compromiterii sau defectarii modulului), introducerea unei perechi de chei intr-un modul de securitate diferit,
- cand este necesara transferarea unei chei private din modulul operational folosit pentru operatii standard ale entitatii, pe un alt modul; situatia poate aparea in cazul defectarii modulului sau in cazul necesitatii distrugerii acestuia.

Introducerea unei chei private intr-un modul de securitate este o operatiune critica si de aceea trebuie implementate masuri si proceduri care sa previna dezvaluirea, modificarea sau falsificarea cheii private.

Introducerea unei chei private intr-un modul hardware de securitate (HSM) al Autoritatilor de Certificare de pe nivelele 0 si 1 de certificare necesita restaurarea cheii de pe carduri in prezenta unui numar corespunzator de detinatori de secret partajat care protejeaza modulul ce contine cheile private.

Deoarece fiecare Autoritate de Certificare poate detine o copie criptata a cheii sale private, cheile pot fi de asemenea transferate intre module.

5.1.1.2.6. Metoda de activare a cheii private

Metodele de activare a cheii private, detinute de diversi utilizatori sau utilizatori ai sistemului AlfaTrust Certification, se refera la activarea cheii inainte de orice folosire a sa, sau de inceperea unei sesiunii de lucru ce necesita folosirea cheii respective (de exemplu, conectarea la Internet). O cheie odata activata poate fi folosita pana la dezactivare.

Executarea procedurilor de activare (si dezactivare) a unei chei private depinde de tipul entitatii care detine cheia respectiva (utilizator final, Autoritate de Inregistrare, Autoritate de Certificare, dispozitiv hardware etc.), de senzitivitatea datelor protejate de cheie si de intervalul de timp in care cheia trebuie sa ramana activa (pe timpul unei singure operatiuni, sesiuni sau pentru o perioada nelimitata).

Toate cheile private ale Autoritatilor de Certificare AlfaTrust Certification de pe nivelele 0 si 1 de certificare, introduse in modul dupa generare, importate sub forma criptata dintr-un alt modul sau restaurate dintr-un secret partajat, raman in stare activa pana la stergerea lor fizica de pe modul sau pana la scoaterea lor din serviciile AlfaTrust Certification. Activarea cheilor private este intotdeauna precedata

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

de autentificarea operatorului. Autentificarea este realizata pe baza unui card criptografic detinut de operator. Dupa introducerea cardului in modulul criptografic si folosirea codului PIN, cheia privata ramane in stare activa pana la scoaterea cardului din modul.

Cheile private ale operatorilor Autoritatii de Inregistrare sunt activate dupa autentificarea operatorului (folosirea codului PIN) si numai pentru durata unei singure operatii criptografice care necesita folosirea cheii respective. Ca urmare a incheierii acestei operatii, cheia privata este dezactivata automat si trebuie reactivata inaintea executarii altei operatii criptografice.

Activarea cheii private a unui utilizator final se face in mod similar cu procedura de activare a cheii private a operatorilor Autoritatii de Certificare, indiferent daca sunt stocate pe un card criptografic sau sub forma criptata, ca fisier pe o discheta sau orice alt mediu de stocare. In cazul utilizatorilor finali persoane juridice (organizatii, institutii etc.) activarea trebuie sa se faca de catre o persoana autorizata a utilizatorului.

5.1.1.2.7. Metoda de dezactivare a cheii private

Metodele de dezactivare a cheii private se refera la dezactivarea cheii dupa folosirea acesteia sau ca urmare a terminarii unei sesiuni in timpul careia a fost folosita cheia.

In cazul unui utilizator final sau al unui operator al Autoritatii de Inregistrare, dezactivarea cheii private de semnatura se face imediat dupa incheierea sesiunii (la iesire din aplicatie). Daca in timpul executarii operatiei criptografice, cheia privata a fost stocata in memoria aplicatiei, aplicatia trebuie sa previna refacerea neautorizata a cheii private. Daca o cheie privata este detinuta de un utilizator persoana juridica, cheia poate fi dezactivata numai de reprezentantul autorizat al acestui utilizator.

In cazul AlfaTrust Certification, dezactivarea unei chei private se face de catre ofiterul de securitate numai in cazul in care o sesiune de lucru a fost incheiata, perioada de validitate a cheii a expirat, cheia a fost revocata sau este necesar sa se suspende imediat activitatile sistemului. Dezactivarea unei chei private se face prin scoaterea cardului din modul.

5.1.1.2.8. Metoda de distrugere a cheii private

Stergerea cheii private a unui utilizator sau operator al Autoritatii de Inregistrare presupune stergerea ei de pe mediul de stocare (discheta, card criptografic, memorie, modul hardware de securitate etc.). Daca o cheie privata apartine unui utilizator persoana juridica, cheia poate fi distrusa numai de catre reprezentantul autorizat al utilizatorului.

Fiecare distrugere de cheie privata este inregistrata in jurnalul de evenimente.

5.1.1.3. Alte aspecte cu privire la managementul perechilor de chei

Cerintelor din acest capitol se refera la procedurile de arhivare a cheii publice si la perioada de validitate a cheilor publice si private ale fiecarui utilizator, inclusiv ale Autoritatilor de Certificare.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.1.1.3.1. Arhivarea cheilor publice

Scopul arhivarii cheilor publice este acela de a crea posibilitatea verificarii semnaturii electronice dupa eliminarea unui certificat din depozit. Acest lucru este foarte important in cazul serviciilor de non-repudiere, cum ar fi serviciul de marca temporala sau serviciul de verificare a starii unui certificat.

Arhivarea cheilor publice presupune arhivarea certificatelor care contin aceste chei.

Fiecare autoritate care emite certificate arhiveaza cheile publice ale utilizatorilor catre care au fost emise certificatele. Cheile publice ale Autoritatii de Certificare sunt arhivate impreuna cu cheile private. Certificatele pot fi, de asemenea, arhivate local de catre utilizatorii finali, in special cand acest lucru este cerut de aplicatiile folosite (de exemplu, sistemele de posta electronica).

Arhivele cheilor publice trebuie protejate in asa fel incat sa se previna adaugarea, inserarea, modificarea si stergerea neautorizata de chei din arhiva. Protectia este realizata prin autentificarea entitatii care face arhivarea si autorizarea cererilor.

Administratorul de securitate verifica lunar integritatea arhivelor de chei publice. Scopul acestei verificari este de a asigura faptul ca nu sunt goluri in arhive si ca certificatele din arhive nu au fost modificate. Mecanismul de verificare a integritatii arhivelor tine cont de faptul ca perioada de pastrare poate fi mai lunga decat cea a mecanismelor de securitate folosite la crearea arhivelor.

Cheile publice sunt pastrate in arhivele cu certificate digitale 15 ani dupa momentul expirarii.

5.1.1.3.2. Perioadele de folosire a cheilor private si publice

Perioada de folosire a cheilor publice este definita de valoarea campului validitate a fiecarui certificat de cheie publica. Exista, de asemenea, si o perioada de validitate a cheii private. Perioada maxima de utilizare a cheilor utilizatorilor nu poate depasi de 2 ori durata de viata a unui certificat. Valorile standard ale perioadei maxime de folosire a certificatelor Autoritatii de Certificare si a certificatelor utilizatorilor fiali sunt dupa cum urmeaza:

- 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 si a cheilor private corespunzatoare poate fi mai scurta in cazul revocarii unui certificat.

In general, data de inceput a validitatii certificatului corespunde cu data emiterii sale. Nu este permisa stabilirea acestei date in trecut sau in viitor.

5.1.1.4. Datele de activare

Datele de activare sunt folosite pentru activarea unei chei private cu care opereaza o Autoritate de Inregistrare, o Autoritate de Certificare, sau un utilizator final. De obicei sunt folosite pentru autorizarea entitatilor si pentru a controla accesul la cheia privata.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.1.1.4.1. Generarea si instalarea datelor de activare

Datele de activare sunt folosite in doua situatii principale:

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

Operatorii Autoritatii de Inregistrare si ai Autoritatilor de Certificare, folosesc parole rezistente la atacuri prin incercari repetate (forta bruta). Se recomanda ca si utilizatorii finali sa foloseasca astfel de parole.

In cazul activarii cheii private, se recomanda sa se foloseasca proceduri de autentificare bazate pe mai multi factori, de exemplu un card criptografic si o fraza de autentificare (passphrase) sau un jeton criptografic (token) si un dispozitiv biometric (de exemplu, cititor de amprente).

Fraza de autentificare mentionata mai sus trebuie generata in concordanta cu cerintele FIPS-112.

5.1.1.4.2. Protectia datelor de activare

Protectia datelor de activare include metodele de control a acestor date prin care se previne dezvaluirea lor. Metodele de control a datelor de activare depind de natura acestora: daca sunt fraze de autentificare sau daca acest control este bazat pe distribuirea informatiilor de activare in secrete partajate. In cazul frazei de autentificare, trebuie impuse recomandarile descrise in FIPS-112, pe cand protejarea secretelor partajate necesita implementarea standardului FIPS-140.

Se recomanda ca datele de activare folosite pentru activarea cheii private sa fie protejate prin controale criptografice si de acces fizic. Datele de activare pot fi datele biometrice sau memorate (nu scrise) de catre entitatea de autentificat. Daca datele de autentificare sunt scrise, nivelul de protectie trebuie sa fie acelasi cu cel al datelor pe care le protejeaza prin folosirea cardului criptografic. Mai multe incercari nereusite de a accesa modulul criptografic trebuie sa duca la blocarea acestuia. Datele de activare stocate nu trebuie sa fie pastrate niciodata impreuna cu cardul criptografic.

5.1.1.4.3. Alte aspecte cu privire la datele de activare

Datele de activare sunt stocate intr-un singur exemplar. Datele de activare care protejeaza accesul la cheia privata stocata pe carduri criptografice pot fi schimbate periodic. Datele de activare fac obiectul arhivarii.

5.1.2. Masuri de securitate fizica, procedurala, de personal si a documentelor

Acest capitol descrie cerintele generale privind securitatea fizica, procedurala si a documentelor, precum si activitatea personalului AlfaTrust Certification in activitatea de generare de chei, verificarea autenticitatii entitatilor, emiterea si publicarea certificatelor, revocarea certificatelor, audit si crearea de copii de siguranta.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.1.2.1. Controale de securitate fizica

Sistemele de calcul, terminalele operatorilor si resursele informationale ale AlfaTrust Certification sunt dispuse intr-o zona dedicata, protejata fizic impotriva accesului neautorizat, distrugerilor sau perturbarii activitatii. Aceste locatii sunt monitorizate. Fiecare intrare si iesire este inregistrata in jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum si temperatura sunt de asemenea monitorizate si controlate.

5.1.2.1.1. Accesul fizic

Accesul fizic in cadrul AlfaTrust Certification este controlat si monitorizat de un sistem de alarma integrat. AlfaTrust Certification dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruziunilor si sisteme de alimentare cu energie electrica in caz de urgenta.

Sediul AlfaTrust Certification si Autoritatea de Inregistrare sunt accesibile publicului in fiecare zi lucratoare intre 10:00 si 16:00. In restul timpului (inclusiv in zilele nelucratoare), accesul este permis numai persoanelor autorizate de catre conducerea AlfaTrust Certification. Vizitatorii locatiilor apartinand AlfaTrust Certification trebuie sa fie insotiti permanent de persoane autorizate.

Zonele ocupate de AlfaTrust Certification se impart in:

* **Zona de securitate clasa I** – nu este permis accesul (nici macar insotit) al nici unei persoane (vizitator, client sau personal al AlfaTrust Certification) cu exceptia administratorilor de securitate si administratorilor de sistem. Persoanele autorizate de a patrunde in aceasta zona de securitate nu vor intra niciodata singure ci vor respecta conditia de acces de minim 2 persoane (“***four eyes or two men rule”***). Aceasta zona de securitate este compusa din:
    - zona serverelor si a echipamentelor de comunicatii,
    - zona administratorilor Autoritatilor de Certificare si a Autoritatii de Validare.

  Zona serverelor este echipata cu un sistem de securitate monitorizat continuu, alcatuit din senzori de miscare, efractie si incendiu. Accesul in aceasta zona este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul Autoritatii de Certificare si administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri si cititoare, montate langa punctul de acces. Fiecare intrare si iesire din zona este inregistrata automat in jurnalul de evenimente.

* **Zona de securitate clasa a II-a** – in aceste zone este permis accesul numai persoanelor autorizate de conducerea AlfaTrust Certification, accesul si activitatea in aceste zone conformandu-se principiului compartimentarii muncii si a principiului nevoii de a cunoaste “***need to know***”. Aceasta zona este compusa din:
    - zona operatorilor Autoritatii de Inregistrare si administratorilor,
    - zona de dezvoltare si testare,
    - zona de depozitare a echipamentelor informatice, de comuncatii sau criptografice.

  Controlul accesului in zona operatorilor si administratorilor se face prin intermediul cardurilor si a cititoarelor de carduri. Deoarece toate informatiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor si administratorilor necesita in prealabil autorizarea acestora, securitatea fizica in aceasta zona este considerata ca fiind adecvata. Cheile de acces pot

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

fi ridicate numai de personalul autorizat. In aceasta zona au acces numai angajatii AlfaTrust Certification si persoanele autorizate; ultimilor nu le este permisa prezenta in zona neinsotiti.

Zona de dezvoltare si testare este protejata intr-o maniera similara cu zona operatorilor si administratorilor. Daca este necesar un altfel de acces, atunci el se poate face numai in prezenta administratorul de securitate. Proiectele in curs de implementare si software-ul aferent este testat in mediul de dezvoltare al AlfaTrust Certification.

* **Zone administrative** – in aceasta categorie intra orice alte zone din locatia Furnizorului de Servicii de Certificare AlfaTrust Certification ce nu se incadreaza in primele doua clase de zone de securitate. In zonele administrative nu este permis accesul vizitatorilor sau a clientilor decat daca sunt insotiti de personal al AlfaTrust Certification. Aceste zone se compun din:
    - birourile personalului,
    - zonele de primire a clientilor AlfaTrust Certification.

5.1.2.1.2. Energie si climatizare

Zona operatorilor si administratorilor, precum si zona de dezvoltare si testare sunt prevazute cu surse de climatizare a mediului ambiental. Din momentul intreruperii alimentarii cu energie, sursele de electricitate de urgenta (UPS) permit continuarea neperturbata a activitatii pana la interventia automata a grupului electrogen ce deserveste toate facilitatile AlfaTrust Certification.

5.1.2.1.3. Expunerea la apa

AlfaTrust Certification si-a luat precautii deosebite pentru a minimiza impactul expunerii la apa a sistemelor AlfaTrust Certification.

5.1.2.1.4. Prevenirea si protectia impotriva incendiilor

AlfaTrust Certification si-a luat precautii deosebite pentru a preveni si a stinge focul sau alte expuneri la flacara sau fum. Masurile AlfaTrust Certification de prevenire si protectie impotriva focului au fost stabilite pentru a respecta reglementarile cu privire la prevenirea si stingerea incendiilor si siguranta la foc.

5.1.2.1.5. Mediile de stocare

Toate mediile in care exista software de productie si date, verificare, arhiva sau informatii salvate se afla in locatiile AlfaTrust Certification sau intr-o locatie off-site de inmagazinare securizata cu controale de acces fizic si logic, pentru a limita accesul numai pentru personalul autorizat si pentru a proteja aceste medii impotriva pagubelor accidentale (cauzate de apa, foc sau camp electromagnetic).

5.1.2.1.6. Aruncarea lucrurilor nefolositoare

Documentele si materialele sensibile sunt distruse (tocate) inainte de a fi aruncate. Mijloacele folosite pentru a strange sau a transmite informatiile sensibile nu mai pot fi citite, inainte de a fi aruncate. Inainte de a fi aruncate, dispozitivele criptografice sunt distruse fizic sau sterse intr-o maniera sigura, in

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

concordanta cu indrumarile anterioare ale producatorului. Alte lucruri nefolositoare sunt aruncate, tinand cont de cerintele AlfaTrust Certification.

5.1.2.1.7. Depozitarea backup-urilor in afara locatiei

Copiile parolelor, codurile PIN si cardurile criptografice sunt stocate in containere speciale, situate in afara locatiei AlfaTrust Certification.

Stocarea in afara locatiei se aplica si in cazul arhivelor, copiilor curente ale informatiilor procesate de sistem si kit-urilor de instalare ale aplicatiilor AlfaTrust Certification. Acest lucru permite refacerea de urgenta a oricarei functii a AlfaTrust Certification in 48 de ore, in locatia principala a AlfaTrust Certification, sau in locatia auxiliara.

5.1.2.2. Controale procedurale

Acest capitol prezinta rolurile ce pot fi atribuite personalului apartinand AlfaTrust Certification, Autoritatii de Inregistrare, utilizatorilor finali si entitatilor partenere. De asemenea, tot in acest capitol sunt descrise responsabilitatile si sarcinile specifice fiecarui rol.

5.1.2.2.1. Functii de incredere

Printre persoanele de incredere se numara toti angajatii, furnizorii si consultantii care au acces la sau controleaza operatiile de autentificare si criptare si care pot influenta:

- Validarea informatiilor din cererile pentru certificate;
- Acceptarea, respingerea sau alte procesari ale cererilor pentru certificate, ale cererilor de revocare, ale cererilor de innoire sau ale informatiilor de inscriere;
- Emiterea sau revocarea certificatelor, inclusiv personalul care are acces la parti restrictionate ale registrului sau;
- Manipularea informatiilor sau cererilor utilizatorului.

Printre persoanele de incredere se numara, dar nu se limiteaza numai la atat:

- Personalul de la serviciu clienti,
- Personalul care se ocupa de operatiile criptografice ale activitatii,
- Personalul de securitate,
- Personalul de la sistemul de administrare,
- Personalul de la departamentul tehnic,
- Directorii care se ocupa cu administrarea facilitatilor si infrastructurii.

In AlfaTrust Certification sunt definite urmatoarele roluri de incredere, care pot fi atribuite uneia sau mai multor persoane:

- ***Administrator de securitate*** = Responsabilitate globala pentru implementarea politicilor si procedurilor de securitate. In plus poate aproba/revoca/suspenda certificate;
  - ✓ initiaza instalarea, configurarea si managementul aplicatiilor software si hardware (inclusiv resursele de retea) ale AlfaTrust Certification;
  - ✓ initiaza si suspenda serviciile oferite de AlfaTrust Certification;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- ✓ coordoneaza administratorii, initiaza si supravegheaza generarea de chei si secrete partajate;
- ✓ atribuie drepturi din punct de vedere al securitatii si privilegiilor de acces ale utilizatorilor;
- ✓ creeaza conturile pentru utilizatorii AlfaTrust Certification;
- ✓ atribuie parole pentru conturile utilizatorilor noi;
- ✓ verifica jurnalele de evenimente;
- ✓ supervizeaza auditurile interne si externe;
- ✓ primeste si raspunde la rapoartele de audit;
- ✓ supervizeaza eliminarea deficientelor constatate in urma auditului;
- ✓ supravegheaza operatorii Furnizorului de Servicii de Certificare;
- ✓ configureaza sistemele si reteaua, activeaza si configureaza mecanismele de protectie a retelei;
- ✓ verifica log-urile de sistem;
- ✓ verifica respectarea Politicii de Certificare si Sigilii Electronice si a DPSI;
- ✓ genereaza secrete partajate si chei;
- ✓ administreaza Lista de Certificate Revocate;
- ✓ creeaza copiile de siguranta;
- ✓ modifica numele si adresele serverelor.

* ***Administratorul de secrete*** = isi desfasoara activitatea la nivelul Autoritatilor de Certificare si Autoritatii de Validare;
  - ✓ supervizeaza si transfera secretele (cheile criptografice si alte date protejate) catre operatorii Autoritatii de Inregistrare;
  - ✓ ia parte la activarea modulului criptografic si la incarcarea cheilor operatorilor (in prezenta acestora);
  - ✓ transfera si activeaza cardurile de identitate ale operatorilor (daca aceste carduri sunt blocate);
  - ✓ mediaza contactele dintre Autoritatea de Inregistrare si Autoritatile de Certificare;
* ***Administratorul de sistem*** = Autorizat sa instaleze, configureze si sa intretina sistemele de incredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification pentru inregistrarea, generarea de certificate, initializarea dispozitivelor si gestiunea revocarilor de certificate;
  - ✓ Instaleaza dispozitivele hardware si sistemele de operare;
  - ✓ instaleaza si configureaza echipamentele de retea;
  - ✓ instaleaza programe;
  - ✓ configureaza sistemul si aplicatiile;
  - ✓ activeaza si configureaza resursele de securitate;
  - ✓ creeaza conturi si parole pentru operatori;
  - ✓ creeaza copii de siguranta si arhiveaza datele;
  - ✓ verifica jurnalele de evenimente (log-uri) si (impreuna cu operatorul Autoritatii de Inregistrare), la ordinul administratorului de secrete, sterge datele in exces.
* ***Operatorul de sistem*** = Responsabil de operarea zilnica a sistemelor de incredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification;
  - ✓ autorizat sa execute operatiile de backup si restaurare a sistemului;
  - ✓ are acces la certificatele utilizatorilor finali;
  - ✓ revoca certificatele utilizatorilor;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- ✓ asigura continuitatea copiilor de siguranta si arhivelor bazelor de date si a crearii log-urilor de sistem;
- ✓ administreaza bazele de date;
- ✓ are acces la informatii confidentiale despre utilizatori, dar nu poate accesa fizic nici o alta resursa a sistemului;
- ✓ transfera copiile de siguranta ale arhivei si ale datelor curente in afara locatiei AlfaTrust Certification.

* ***Operatorii Autoritatii de Inregistrare*** = isi desfasoara activitatea in zona de securitate clasa a II-a si in zonele administrative de la nivelul Autoritatii de Inregistrare;
  - ✓ verifica identitatea solicitantilor de certificate si corectitudinea cererilor primite;
  - ✓ emit confirmari ale cererilor pe care le trimit Autoritatii de Certificare;
  - ✓ genereaza cheile si iau parte la generarea certificatelor, trimitand informatiile din cerere la o Autoritate de Certificare;
  - ✓ arhiveaza (sub forma de documente pe hartie) cererile si confirmarile emise, care fac obiectul stergerii, la ordinul administratorului de secrete si in prezenta acestuia,
* ***Auditorul de sistem*** = autorizat sa acceseze arhivele si log-urile de audit ale sistemelor de incredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification. Responsabil de efectuarea de audituri interne pentru respectarea DPSI si a Politicilor de Certificare, Sigilii Electronice si Marcare Temporala de catre Furnizorul de Servicii de Certificare; aceasta responsabilitate se extinde si asupra Autoritatii de Inregistrare care opereaza in cadrul AlfaTrust Certification.
* ***Administratorul depozitului*** = isi desfasoara activitatea la nivelul Autoritatii de Validare si administreaza directoarele AlfaTrust Certification disponibile publicului, creeaza si actualizeaza continutul directoarelor din depozit, creeaza paginile web si administreaza legaturile (link-urile).

5.1.2.2.2. Numarul de persoane necesare pentru fiecare sarcina

Procesul de generare de chei – pentru semnarea certificatelor si al CRL-urilor – este una din operatiile ce necesita o atentie deosebita. Generarea necesita prezenta a cel putin doua persoane: un administrator de securitate si un administrator de sistem. Procesul de generare a cheii Autoritatii de Certificare poate fi de asemenea observat de catre posesori de secrete partajate care pastreaza partea lor de cheie in locatii sigure.

Prezenta administratorului de securitate, a administratorului Autoritatii de Certificare si a unui numar corespunzator de posesori de secrete partajate este necesara si la incarcarea cheii criptografice a Autoritatii de Certificare in modulul hardware de securitate (HSM). Incarcarea cheii criptografice a Autoritatii de Inregistrare in modulul hardware de securitate (daca este cazul) necesita prezenta administratorului de secrete si a unui operator al Autoritatii de Inregistrare.

Orice alta operatiune sau rol, descris in cadrul DPSI-ului sau care are legatura cu un utilizator final, poate fi efectuata de o singura persoana, special desemnata in acest sens.

5.1.2.2.3. Identificarea si autentificarea pentru fiecare rol

Personalul AlfaTrust Certification este supus identificarii si autentificarii in urmatoarele situatii:

- plasarea pe lista de persoane care au dreptul de a accesa locatiile AlfaTrust Certification ,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- plasarea pe lista de persoane care au acces fizic la sisteme si resurse de retea apartinand AlfaTrust Certification,
- emiterea confirmarii care autorizeaza indeplinirea rolului asignat,
- asignarea unui cont si a unei parole in sistemul informatic al AlfaTrust Certification.

Fiecare cont desemnat:

- trebuie sa fie unic si desemnat direct unei anumite persoane,
- nu poate fi folosit in comun cu nici o alta persoana,
- trebuie restrictionat conform functiei (ce reiese din rolul indeplinit de persoana respectiva) pe baza software-ului de sistem al AlfaTrust Certification, a sistemului de operare si a controalelor de aplicatii.

5.1.2.3. Controale de personal

AlfaTrust Certification garanteaza ca se asigura ca persoana care indeplineste responsabilitatile functiei, conform cu rolul atribuit in cadrul unei Autoritati de Certificare, Validare sau Inregistrare:

- ✓ a absolvit cel putin liceul,
- ✓ este cetatean roman,
- ✓ a semnat un contract care descrie rolul si responsabilitatile sale in cadrul sistemului,
- ✓ a beneficiat de un stagiu de pregatire avansata in conformitate cu obligatiile si sarcinile asociate functiei sale,
- ✓ a fost instruit cu privire la protectia datelor personale si informatiilor confidentiale sau private,
- ✓ a semnat un contract ce contine clauze referitoare la protejarea informatiilor senzitive (din punctul de vedere al securitatii AlfaTrust Certification) si a datelor confidentiale si private ale utilizatorilor finali,
- ✓ nu indeplineste sarcini care pot genera conflicte de interese intre Autoritatea de Certificare si Autoritatea de Inregistrare care actioneaza in numele acesteia.

5.1.2.3.1. Cerinte privind trecutul, calificarile si experienta

Personalul care doreste sa se numere printre persoanele de incredere din AlfaTrust Certification trebuie sa prezinte dovada indeplinirii cerintelor legate de trecut, calificari si experienta, necesare pentru a indeplini in mod competent si satisfacator responsabilitatile postului respectiv, precum si dovada oricaror acceptari guvernamentale, daca exista, necesare pentru a indeplini servicii de certificare in baza unor contracte guvernamentale. Verificarea informatiilor cu privire la personal se repeta la cel putin 5 ani pentru personalul care ocupa pozitii de incredere.

Inainte de inceperea serviciului intr-o functie de incredere, AlfaTrust Certification face verificari asupra informatiilor cu privire la personal, cuprinzand urmatoarele:

- Confirmarea locului de munca anterior;
- Verificarea referintelor profesionale;
- Confirmarea celei mai inalte sau relevante institutii de invatamant urmate;
- Solicitarea cazierului judiciar;
- Solicitarea rapoartelor financiare;
- Solicitarea rapoartelor privind permisul de conducere;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- Solicitarea rapoartelor privind asistenta sociala.

In masura in care, oricare dintre cerintele impuse de aceasta sectiune, nu poate fi satisfacuta din cauza unei interziceri sau limitari din legea locala sau din cauza altor circumstante, AlfaTrust Certification S.A. va folosi o tehnica de investigatie care este permisa de lege si care furnizeaza informatii asemanatoare, inclusiv, dar nu limitandu-se la, obtinerea unei verificari a trecutului, realizata de agentia guvernamentala adecvata.

Factorii implicati in verificarea trecutului, ce pot duce la respingerea candidatilor pentru functiile de incredere sau la luarea de masuri impotriva celor care fac parte deja dintre persoanele de incredere, includ in general urmatoarele:

- Prezentarea gresita a informatiilor cerute facuta de catre candidat sau de catre persoana de incredere;
- Referinte personale nefavorabile sau care nu inspira incredere;
- Condamnari penale;
- Indicii ale lipsei de responsabilitate financiara.

Rapoartele care contin astfel de informatii sunt evaluate de personalul de la resurse umane si securitate, care determina cursul potrivit al actiunii, in functie de tipul, importanta si frecventa comportamentului dezvaluit de verificarea trecutului. Aceste actiuni pot include masuri care pot ajunge la anularea ofertelor de angajare pentru candidatii la functii de raspundere sau la scoaterea din functie a persoanelor de incredere.

Folosirea informatiilor gasite prin verificarea trecutului pentru a intreprinde astfel de actiuni este supusa reglementarilor in vigoare din Romania.

5.1.2.3.2. Cerinte de pregatire

AlfaTrust Certification S.A. asigura personalului pregatirea necesara pentru a indeplini in mod competent si satisfacator responsabilitatile functiei. AlfaTrust Certification S.A. trece in revista periodic si intensifica programele de pregatire, atunci cand este nevoie.

Programele de pregatire ale AlfaTrust Certification S.A. sunt realizate tinand cont de responsabilitatile individuale si includ urmatoarele:

- Concepte de baza despre infrastructura cheii publice (PKI);
- Responsabilitatile functiei;
- Politicile si procedurile de securitate si operationale ale AlfaTrust Certification S.A.;
- Folosirea si functionarea hardware-ului si software-ului existent;
- Raportarea si tratarea cazurilor de incident si compromis;
- Procedurile de recuperare in caz de dezastru si de continuare a activitatii.

5.1.2.3.3. Cerintele si frecventa cursurilor de perfectionare

AlfaTrust Certification S.A. furnizeaza cursuri de perfectionare si de actualizare pentru personal, in masura si cu frecventa care permit asigurarea mentinerii nivelului necesar pentru indeplinirea competenta si satisfacatoare a responsabilitatilor de serviciu. Se asigura periodic pregatire de securitate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

5.1.2.3.4. Sanctiuni pentru actiuni neautorizate

Se iau masuri disciplinare adecvate pentru actiunile neautorizate sau pentru alte violari ale politicilor si procedurilor AlfaTrust Certification S.A. Actiunile disciplinare pot include masuri care duc pana la incetarea contractului si sunt luate in functie de frecventa si severitatea actiunilor.

5.1.2.3.5. Cerinte pentru contractarea personalului

In circumstante limitate, se pot folosi contractanti sau consultanti independenti pentru a ocupa functii de incredere. Orice astfel de contractant sau consultant este mentinut dupa aceleasi criterii functionale si de securitate care se aplica si in cazul angajatilor AlfaTrust Certification, care se afla intr-o pozitie asemanatoare.

Contractantii si consultantii independenti care nu au desavarsit procedurile de verificare a trecutului specificate la punctul 5.1.2.3.1 pot accesa locatiile securizate ale AlfaTrust Certification numai daca sunt escortati si supravegheati direct de persoane de incredere.

5.1.2.3.6. Documentatie furnizata personalului

Personalul AlfaTrust Certification implicat in functionarea serviciilor infrastructurii cheii publice ale AlfaTrust Certification trebuie sa citeasca, sa inteleaga si sa-si insuseasca acest set de practici si proceduri si politica de securitate a AlfaTrust Certification. AlfaTrust Certification S.A. ofera angajatilor sai pregatirea necesara si alta documentatie necesara pentru a indeplini competent si satisfacator responsabilitatile functiei.

5.2. Controale CompuSEC

Sarcinile angajatilor, colaboratorilor sau entitatilor partenere Furnizorului de Servicii de Certificare care lucreaza in mediul AlfaTrust Certification sunt realizate prin intermediul unor dispozitive hardware (sisteme informatice si de comunicatii, dispozitive criptografice, etc.) si aplicatii software de incredere.

5.2.1. Cerintele de securitate specifice

Cerintele tehnice prezentate in acest capitol se refera la controalele de securitate specifice calculatoarelor, retelelor de calculatoare si aplicatiilor folosite in mediul AlfaTrust Certification. Masurile de securitate care protejeaza sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicatiilor precum si din punct de vedere fizic.

Calculatoarele apartinand FSC-ului si componentelor asociate acestora au implementate urmatoarele masuri (controale) de securitate:

- autentificarea obligatorie la nivelul sistemului de operare si al aplicatiilor,
- control discretionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securitatii,
- calculatorul este accesibil doar personalului autorizat, cu roluri de incredere in AlfaTrust Certification ,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- separarea sarcinilor, conform rolului in cadrul sistemului,
- identificarea si autentificarea rolurilor si a personalului care indeplineste aceste roluri,
- prevenirea refolosirii unui obiect de catre un alt proces dupa eliberarea acestuia de catre procesul autorizat,
- protectia criptografica a schimburilor de informatii si protectia bazelor de date,
- arhivarea istoricului operatiunilor executate pe un calculator si a datelor necesare auditarii,
- o cale sigura ce permite identificarea si autentificarea rolurilor si a personalului care indeplineste aceste roluri,
- metode de restaurare a cheilor (numai in cazul modulelor hardware de securitate), a aplicatilor si a sistemului de operare,
- mijloace de monitorizare si alertare in cazul accesului neautorizat la resursele de calcul.

5.2.2. Controale pentru managementul securitatii informatiei

Scopul controalelor pentru managementului securitatii este acela de a superviza functionalitatea sistemelor AlfaTrust Certification, garantand astfel ca acestea opereaza corect si in concordanta cu configurarea acceptata si implementata.

Configuratia curenta a sistemelor AlfaTrust Certification, precum si orice modificare si actualizare a acestora, este inregistrata si controlata.

Controalele aplicate sistemelor AlfaTrust Certification permit verificarea continua a integritatii aplicatiilor, versiunii si autentificarea si verificarea originii dispozitivelor hardware.

Fiecare aplicatie, inainte de a fi folosita in productie de AlfaTrust Certification, este instalata astfel incat sa se permita controlul versiunii curente si sa se previna instalarea neautorizata de programe sau falsificarea celor existente.

Reguli similare se aplica in cazul inlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate in asa fel incat sa poata fi urmarita si evaluata ruta fiecaruia, pana la locul sau de instalare,
- livrarea unui dispozitiv fizic pentru inlocuire se realizeaza intr-un mod similar celui de livrare al dispozitivului original; inlocuirea se realizeaza de catre personal calificat si de incredere.

5.2.3. Controale de securitate a retelei

Serverele si statiile de lucru de incredere apartinand AlfaTrust Certification sunt conectate prin intermediul unei retele locale (LAN), divizate in mai multe subretele, cu acces controlat. Accesul dinspre Internet catre orice segment, este protejat prin intermediul unui firewall inteligent.

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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.3. Inregistrarea evenimentelor si procedurile de auditare

Pentru a gestiona eficient sistemele AlfaTrust Certification si pentru a putea audita actiunile utilizatorilor si personalului AlfaTrust Certification, toate evenimentele care apar in sistem sunt inregistrate. Informatiile inregistrate alcatuiesc jurnalele (log-urile) de evenimente si trebuie pastrate in asa fel incat sa permita Entitatilor Partenere sa acceseze informatiile corespunzatoare si necesare rezolvarii disputelor, sau sa detecteze tentativele de compromitere a securitatii AlfaTrust Certification. Evenimentele inregistrate fac obiectul procedurilor de arhivare. Arhivele sunt pastrate in afara incintei AlfaTrust Certification.

Cand este posibil, log-urile sunt create automat. Daca inregistrarile nu pot fi create automat, se vor folosi jurnalele de evenimente pe hartie. Fiecare inregistrarea in log, electronic sau de mana, este pastrata si dezvaluita atunci cand se desfasoara un audit.

In sistemele AlfaTrust Certification, auditorul intern de securitate este obligat sa realizeze anual un audit referitor la respectarea reglementarilor acestei DPSI de catre mecanismele si procedurile implementate si sa evalueze eficienta procedurilor de securitate existente.

Log-urile de evenimente AlfaTrust Certification contin inregistrari ale tuturor activitatilor generate de componentele software din cadrul sistemului. Aceste inregistrari sunt impartite in trei categorii separate:

- ✓ *inregistrari de sistem* – contin informatii despre cererile clientilor si raspunsurile serverului (sau invers) la nivelul protocolului de retea (de exemplu http, https); datele concrete care se inregistreaza sunt: adresa IP a statiei sau a server-ului, operatiunile executate (de exemplu: cautare, editare, scriere etc.) si rezultatele lor (de exemplu introducerea cu succes a unei inregistrari in baza de date),
- ✓ *erori* – contine informatii despre erori la nivelul protocoalelor de retea si la nivelul modulelor aplicatiilor,
- ✓ *audit* – contin informatii specifice serviciilor de certificare, de exemplu: cererea de inregistrarea si de certificare, acceptarea certificatului, emiterea de certificat si CRL etc.

Inregistrarile din jurnalul de evenimente sunt revazute in detaliu cel putin o data pe luna. Orice eveniment avand o importanta semnificativa este explicat si descris intr-un jurnal.

Inregistrarile evenimentelor sunt stocate in fisiere pe discul sistem pana cand acestea ajung la capacitatea maxima permisa. In tot acest timp sunt disponibile on-line, la cererea fiecarei persoane, sau proces autorizat. Dupa depasirea spatiului alocat, jurnalele sunt pastrate in arhive si pot fi accesate numai off-line, de la o anumita statie de lucru.

Jurnalele arhivate sunt pastrate cel putin 2 ani.

5.4. Arhivarea inregistrarilor

Este necesar ca toate datele si fisierele referitoare la informatiile despre securitatea sistemului, cererile trimise de utilizatori, informatiile despre utilizatori, certificatele emise si CRL-urile, cheile folosite de Autoritatile de Certificare si Inregistrare, si toata corespondenta dintre AlfaTrust Certification si utilizatorii finali sa fie arhivate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

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

Arhivele off-line contin certificate (inclusiv certificatele revocate) expirate cu pana la 10 ani inainte de data curenta. Arhiva certificatelor revocate contine informatii despre certificatul identificat, motivul revocarii, daca si cand a fost certificatul plasat in CRL. Arhiva este folosita pentru rezolvarea eventualelor dispute, referitoare la documente vechi, semnate electronic de un utilizator.

Pe baza arhivelor se creeaza copiile de siguranta care sunt tinute in afara locatiei AlfaTrust Certification.

5.4.1. Tipurile de date arhivate

Urmatoarele date sunt incluse in procesul de arhivare:

- informatiile rezultate in urma examinarii si evaluarii (ca urmare a unui audit) masurilor de protectie logice si fizice ale unei Autoritati de Certificare, Autoritatii de Inregistrare si Autoritati de Validare,
- cererile primite si deciziile emise, in forma electronica, trimise de, sau catre un utilizator sub forma de fisiere sau mesaje electronice,
- baza de date cu utilizatorii finali,
- baza de date cu certificate,
- Listele de Certificate Revocate emise,
- istoria cheii Autoritatii de Certificare, de la generare pana la distrugere,
- istoria cheilor utilizatorilor finali, de la generare pana la distrugere, daca cheia se arhiveaza in baza de date a Autoritatii de Certificare.

5.4.2. Frecventa arhivarii datelor

Arhivarea datelor se realizeaza pe mai multe nivele, astfel:

- baza de date cu certificate si baza de date cu utilizatori finali sunt pastrate pe mediile AlfaTrust Certification pentru o perioada de 3 ani (din momentul emiterii certificatului). Pentru urmatorii 3 ani, arhivele sunt stocate pe benzi magnetice sau CD-uri, ramanand in continuare disponibile on-line. In al saptelea an (la sase ani dupa emiterea de certificatului) toate informatiile despre utilizatori si certificatele acestora sunt stocate pe CD-uri si sunt disponibile off-line,
- CRL, corespondenta electronica si cererile trimise de utilizatori precum si deciziile emise sunt arhivate in acelasi mod si cu aceeasi frecventa ca si bazele de date cu certificate si utilizatori,
- cheile Autoritatilor de Certificare, Inregistrare si Validare sunt stocate – dupa expirarea certificatelor asociate – pe medii ce nu pot fi suprascrise si criptate cu cheia controlata de administratorul de securitate; cheile astfel arhivate sunt disponibile numai off-line.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

5.4.3. Perioada de pastrare a arhivelor

Datele arhivate (sub forma electronica sau pe hartie), sunt pastrate pentru o perioada de timp de 15 ani. Dupa expirarea perioadei de pastrare declarate, datele arhivate sunt distruse.

5.4.4. Cerintele pentru marcarea temporala a inregistrarilor

Datele arhivate sunt semnate cu o marca temporala, creata de Autoritatea de Marcare Temporala (TSA) autorizata, avand certificatul emis de Autoritatea de Certificare operationala afiliata la AlfaTrust Certification CA. Serviciul de marcare temporala este disponibil in cadrul AlfaTrust Certification S.A.

5.5. Procedura de backup si restaurare

Copiile de siguranta permit restaurarea completa (daca este necesar, de exemplu, dupa distrugerea sistemului) a datelor esentiale pentru activitatea AlfaTrust Certification. Pentru a realiza acest lucru, sunt copiate urmatoarele aplicatii si fisiere:

- discurile de instalare a aplicatiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicatiilor pentru Autoritatile de Certificare, Inregistrare si Validare,
- serverul web,
- istoricul cheilor, certificatelor si CRL-urilor autoritatilor,
- datele din depozit,
- datele privind utilizatorii finali si personalul AlfaTrust Certification,
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influenta deosebita asupra timpului si costului restaurarii sistemelor Furnizorului de Servicii de Certificare dupa defectarea, sau distrugerea sistemului. AlfaTrust Certification foloseste atat back-up-uri totale (saptamanale), cat si back-up-uri incrementale (zilnice), toate copiile sunt clonate si clonele sunt pastrate in alta locatie, in aceleasi conditii de securitate ca si cele din locatia primara.

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

5.6. Compromiterea securitatii cheii si recuperarea in caz de dezastru

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

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

5.6.1. Compromiterea resurselor de calcul, a aplicatiilor software si/sau datelor

Politica de securitate a AlfaTrust Certification ia in considerare urmatoarele amenintari ce pot influenta disponibilitatea si continuitatea serviciilor oferite:

- distrugerea fizica a sistemului de calcul al AlfaTrust Certification, inclusiv a resurselor de retea – aceasta amenintare se refera la distrugerile provocate de situatiile de urgenta,
- functionarea defectuoasa a aplicatiilor, avand ca efect imposibilitatea accesarii datelor - aceste deteriorari se refera la sistemul de operare, aplicatiile utilizatorilor si executarea de aplicatii periculoase, cum ar fi virusii, viermii, caii troieni,
- pierderea unor servicii de retea importante pentru activitatea AlfaTrust Certification . Acestea se refera in primul rand la caderile de tensiune si distrugerea legaturilor de retea,
- distrugerea unei parti din Intranetul folosit de AlfaTrust Certification pentru a furniza servicii – acest lucru poate duce la obstructionarea clientilor si refuzul (neintentionat) serviciilor.

Pentru a preveni sau limita efectele amenintarilor de mai sus:

- Politica de securitate a AlfaTrust Certification include un Plan de continuitate a afacerii si recuperare in caz de dezastru,
- In cazul aparitiei unui eveniment ce blocheaza functionarea AlfaTrust Certification, in maxim 48 de ore, va fi activata locatia auxiliara ce poate substitui toate functiile importante ale unei Autoritatii de Certificare pana la restaurarea locatiei principale. Distanta dintre locatia primara si cea secundara este suficienta pentru ca majoritatea potentialelor dezastre care pot afecta locatia primara sa nu afecteze in acelasi timp si locatia secundara,
- Instalarea de versiuni noi ale aplicatiilor software in productie se poate face numai dupa testarea intensiva a acestora intr-un mediu de test, in conformitate cu procedurile descrise. Orice modificare a sistemului necesita aprobarea administratorului de securitate al AlfaTrust Certification,
- Sistemul AlfaTrust Certification dispune de aplicatii pentru crearea copiilor de backup pe baza carora se poate face in orice moment restaurarea sistemului si auditarea acestuia. Copiile de siguranta includ toate datele relevante din punct de vedere al securitatii.

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

In cazul compromiterii cheii private a unei Autoritati de Certificare (afiliata la AlfaTrust Certification), sau in cazul suspiciunii unei astfel de compromiteri, trebuie luate urmatoarele masuri:

- Autoritatea de Certificare genereaza o noua pereche de chei si un nou certificat,
- toti utilizatorii de certificate sunt informati imediat despre compromiterea cheii private prin intermediul mass-media sau postei electronice,
- certificatul corespunzator cheii compromise va fi pus in Lista de Certificate Revocate,
- toate certificatele din calea de certificare a certificatului compromis sunt revocate, specificandu-se motivul revocarii,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- se genereaza noi certificate pentru utilizatorii finali,
- noile certificate sunt trimise utilizatorilor in mod gratuit.

Dupa fiecare recuperare a sistemului ca urmare a unui dezastru, administratorul de securitate sau administratorul de sistem va actiona in conformitate cu Planul de continuitate a afacerii si recuperare in caz de dezastru.

6. Profilele certificatelor, a listei de revocare a certificatelor si a protocolului de verificare on-line a starii certificatului

Profilul certificatelor si al Listei de Certificate Revocate (CRL) respecta formatul descris in standardul ITU-T X.509 v.3, in timp ce profilul OCSP respecta cerintele RFC 2560. Informatiile de mai jos descriu semnificatia campurilor din certificat, CRL si OCSP, standardul aplicat si extensiile folosite de AlfaTrust Certification.

6.1. Profilul certificatelor

Conform standardului X.509 v.3, un certificat este alcatuit din urmatoarea secventa de campuri:

- corpul certificatului (***tbscertificate***),
- informatii despre algoritmul folosit pentru semnarea certificatului (***signatureAlgorithm***),
- semnatura electronica propriu-zisa a Autoritatii de Certificare (***signatureValue***).

6.1.1. Continutul certificatului

Continutul certificatului include campuri de baza si extensii (*standard* - descrise de norme si *private* – definite de autoritatea emitenta).

Extensiile definite intr-un certificat conform normelor permit adaugarea de atribute suplimentare specifice utilizatorului final si cheii publice si simplifica managementul structurii ierarhice a certificatului. Certificatele emise in conformitate cu standardul X.509 v.3 permit definirea unor extensii proprietare, unice pentru o implementare data.

6.1.1.1. Campurile de baza

Certificatele AlfaTrust Certification contin urmatoarele campuri de baza:

- ***Version***: a treia versiune (X.509 v.3) a formatului de certificat,
- ***SerialNumber***: numarul serial al certificatului, unic in cadrul domeniului Autoritatii de Certificare,
- ***signatureAlgorithm***: identificatorul algoritmului de semnatura folosit de Autoritatea de Certificare emitenta, poate fi, dupa caz:
  - md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) sau
  - sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) sau sha256WithRSAEncryption
- ***Issuer***: numele distinctiv (ND) al Autoritatii de Certificare,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- ***Validity***: perioada de validitate, descrisa prin intermediul unei date de incepere (***notBefore***) si a unei date de expirare (***notAfter***) a certificatului, in baza sistemului universal de referinta temporala (Universal Time Coordinated). AlfaTrust Certification poseda un ceas controlat de Atomic Frequency Standard,
- ***Subject***: numele distinctiv (ND) al utilizatorului final care este subiectul certificatului. Numele distinctiv respecta cerintele standardului X.501. Valorile unora dintre atributele acestor campuri sunt optionale,
- ***SubjectPublicKeyInfo***: valoarea cheii publice impreuna cu identificatorul algoritmului criptografic folosit. Criptat in conformitate cu RFC 3280, poate contine informatii despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, marimea cheii in biti si valoarea cheii publice).

6.1.1.2. Extensiile standard ale certificatelor

Rolul fiecarei extensii este definit de valoarea standard a identificatorului de obiect folosit (Object Identifier - OID). Extensia, functie de optiunea autoritatii emitente, poate fi critica sau non-critica. Daca o extensie este definita ca fiind critica, aplicatia care foloseste certificatul trebuie sa respinga orice certificat care contine o extensie critica nerecunoscuta. Pe de alta parte, extensiile definite ca fiind non-critice pot fi omise.

AlfaTrust Certification accepta urmatoarele campuri de extensii standard:

- ✓ ***AuthorityKeyIdentifier***: identificatorul certificatului de cheie publica al Autoritatii de Certificare, asociat cheii private folosita pentru semnarea certificatelor – aceasta extensie nu este critica,
- ✓ ***SubjectKeyIdentifier*** – identificatorul cheii subiectului - aceasta extensie nu este critica,
- ✓ ***KeyUsage***: scopul in care poate fi folosita cheia - aceasta extensie este critica. Extensia descrie pentru ce poate fi utilizata o cheie, de exemplu, pentru criptarea de date, pentru schimbul de date, pentru semnatura electronica, etc.:
  - *digitalSignature (0)* – cheie pentru crearea de semnaturi electronice,
  - *nonRepudiation (1)* – cheie asociata cu serviciile de ne-repudiere,
  - *keyEncipherment (2)* – cheie pentru schimbul de chei,
  - *dataEncipherment (3)* – cheie pentru criptarea datelor,
  - *keyAgreement (4)* – cheie pentru negocierea de chei,
  - *keycertsign (5)* – cheie pentru semnarea de certificate,
  - *cRLSign(6)* – cheie pentru semnarea de CRL-uri,
  - *encipherOnly (7)* – cheie numai pentru criptare,
  - *decipherOnly (8)* – cheie numai pentru decriptare.
- ✓ ***ExtKeyUsage***: defineste restrictiile cu privire la folosirea cheii (RFC 3280 si predecesorii) - extensia nu este critica. Acest camp defineste unul sau mai multe domenii de utilizare posibila a certificatului, aditional domeniilor standard, definite de campul *KeyUsage*. Acest camp trebuie inteles ca o restrangere a scopurilor permise definite in campul *KeyUsage*. AlfaTrust Certification emite certificate care pot contine una dintre urmatoarele valori sau o combinatie de astfel de valori in campul *ExtKeyUsage*:
  - *serverAuth* – autentificarea severelor web SSL/TLS; *KeyUsage* are setati bitii pentru:
    - *digitalSignature*, *keyEncipherment* sau *keyAgreement*;
  - *clientAuth* – autentificarea clientilor web SSL/TLS; *KeyUsage* are setati bitii pentru:
    - *digitalSignature* si /sau *keyAgreement*;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- *codeSigning* – semnarea codurilor executabile; *KeyUsage* are setat bitul pentru
  - *digitalSignature*;
- *emailProtection* – protectia e-mail-ului; *keyUsage* are setati bitii pentru:
  - *digitalSignature*, *nonRepudiation* si/sau (*keyEncipherment* sau *keyAgreement*),
- *ipsecEndSystem* – protocolul de autentificare si/sau criptare IPSec,
- *ipsecTunnel* – protocolul IPSec Tunnelling,
- *ipsecUser* – protocolul de protectie IPSec al aplicatiilor utilizatorului,
- *timeStamping* – legarea rezumatului (digest) cu timpul furnizat de sursa de incredere; *KeyUsage* are setati bitii pentru:
  - *digitalSignature*, *nonRepudiation*.
- *ocspSigning* – asigneaza dreptul de a emite confirmari privind starea certificatului in numele AC-ului; *KeyUsage* are setati bitii pentru:
  - *digitalSignature*, *nonRepudiation*.
- *dvcs* – emiterea unei confirmari de catre un notar autorizat, pe baza protocolului DVCS (RFC 3029 - Data Validation and Certification Server Protocols); *KeyUsage* are setati bitii pentru:
  - *digitalSignature*, *nonRepudiation*, *cRLSign*.
- *EncryptedFileSystem* – permite folosirea certificatului pentru criptarea sistemului de fisiere (EFS); este cerut obligatoriu de anumite aplicatii de acest gen (ex. EFS);
- *SmartCardLogon* – permite utilizarea certificatului pentru operatia de „smartcard logon" - autentificare in sistemul de operare, bazata pe certificat digital;

✓ ***CertificatePolicies*** – extensia indica politica (politicile) sub care va emite certificate o Autoritate de Certificare sau politica (politicile) sub care a fost emis un certificat de catre o Autoritate de Certificare. Extensia este o lista de *PolicyInformation* – informatii (identificatorul, adresa electronica) despre o politica de certificare aplicata. Aceasta extensie nu este critica.

Certificate emise de catre Autoritatile de Certificare AlfaTrust Certification includ si calificatori recomandati de RFC 3280:

* ***PolicyMapping***: map-area politicii – acest camp nu este critic; acest camp contine una sau mai multe perechi de OID, definind echivalenta politicii emitentului certificatului cu politica subiectului certificatului,
* ***SubjectAlternativeName***: numele alternativ al subiectului – acest camp nu este critic,
* ***BasicConstraints***: constrangeri de baza – indica tipul certificatului (certificat de AC sau entitate finala), precum si lungimea maxim admisa pentru lantul de certificate – acest camp este critic,
* ***CRLDistributionPoints***: punctul de distribuire a Listei Certificatelor Revocate – acest camp nu este critic; extensia defineste adresa din retea la care se afla CRL-ul curent al Autoritatii emitente a certificatului in cauza,
* ***AuthorityInfoAccessSyntax***: accesul la informatiile despre Autoritatea de Certificare – acest camp nu este critic; campul indica metoda de informare si furnizare a serviciilor de catre emitentul certificatului,
* ***OCSPNoCheck***: daca este prezenta in cadrul unui certificat al unui responder OCSP, clientii care primesc raspunsuri OCSP semnate cu o cheie privata asociata certificatului pot avea incredere cu privire la starea acestui certificat pe perioada sa de valabilitate, aceasta extensie este non-critica si este definita de standardul RFC 2560,
* ***NetscapeCertType***: aceasta extensie limiteaza utilizarea certificatului numai la anumite aplicatii specificate de valoarea extensiei. Daca nu este prezenta, certificatul poate fi folosit pentru orice

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Operator de date cu caracter personal cu nr. 18195

aplicatie cu exceptia aplicatiilor de *ObjectSigning*. Extensia este necritica, iar valoarea sa poate fi o combinatie din urmatoarele:

- *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 clienti de mail securizat S/MIME,
- *ObjectSigning* (bit 3) - certificatul poate fi folosit pentru semnarea obiectelor cum ar fi apleturi Java sau plugin–uri,
- *SSL CA* (bit 5) - certificatul poate fi folosit pentru emiterea de certificate utilizate pentru SSL,
- *S/MIME CA* (bit 6) - certificatul poate fi folosit pentru emiterea de certificate utilizate pentru S/MIME,
- *ObjectSigning CA* (bit 7) – certificatul poate fi folosit pentru emiterea de certificate utilizate pentru ObjectSigning,

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

Certificatele emise de catre AlfaTrust Certification pot contine diferite combinatii ale extensiilor definite in cadrul acestui subcapitol.

6.1.2. Identificatorul algoritmului de semnare

Campul ***signatureAlgorithm*** contine identificatorul algoritmului criptografic folosit pentru semnarea electronica a certificatului de catre Autoritatea de Certificare. In cazul AlfaTrust Certification este folosit algoritmul RSA, in combinatie cu functia hash SHA-1 sau SHA-256.

6.1.3. Campul ce contine semnatura electronica

Valoarea campului ***signatureValue*** este rezultatul aplicarii functiei de hash asupra tuturor campurilor certificatului (*tbscertificate*) si a algoritmului de semnare a rezumatului obtinut, folosind cheia privata a autoritatii.

6.2. Profilul listei de certificate revocate (CRL)

Lista de Certificate Revocate (CRL) consta din trei campuri;

- primul camp (***tbscertList***) contine informatii despre certificatele revocate,
- al doilea (***signatureAlgorithm***) - informatii despre identificatorul algoritmului folosit pentru semnarea listei,
- al treilea (***signatureValue***) contine semnatura electronica a Autoritatii de Certificare.

Campul *tbscertList* este o secventa de campuri obligatorii si optionale. Campurile obligatorii identifica emitentul CRL-ului in timp ce campurile optionale contin informatii despre certificatele revocate si extensiile CRL-ului.

Continutul campurilor obligatorii si optionale dintr-un CRL sunt urmatoarele:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

- ✓ ***Version***: versiunea formatului de CRL,
- ✓ ***Signature***: identificatorul algoritmului folosit de Autoritatea de Certificare pentru a semna CRL-ul; autoritatile AlfaTrust Certification semneaza CRL-urile folosind algoritmul ***sha1WithRSAEncryption***, sau ***sha256WithRSAEncryption***.
- ✓ ***Issuer***: numele Autoritatii de Certificare care a emis CRL-ul; fiecare autoritate a AlfaTrust Certification emite propria sa Lista de Certificate Revocate,
- ✓ ***ThisUpdate***: data publicarii CRL-ului,
- ✓ ***NextUpdate***: date la care se va publica urmatorul CRL; daca campul este prezent, valoarea sa descrie data maxima pana la care se va face actualizarea CRL-ului,
- ✓ ***RevokedCertificates***: lista certificatelor revocate (campul este gol in cazul in care nu a fost revocat nici un certificat); informatia consta din trei sub-campuri:
  - *usercertificates* – numarul serial al certificatului revocat,
  - *revocationDate* – data revocarii certificatului,
  - *crlEntryExtensions* – contine informatii suplimentarea despre certificatele revocate - optional.
- ✓ ***crlExtensions***: informatii suplimentare despre Lista de Certificate Revocate (camp optional). Dintre extensiile posibile, cele mai importante sunt urmatoarele:
  - *AuthorityKeyIdentifier* - care permite identificarea cheii publice corespunzatoare cheii private folosita pentru semnarea listei si
  - *cRLNumber*, care contine un numar serial incrementat monoton al listei emisa de Autoritatea de Certificare (prin intermediul acestei extensii, utilizatorul are posibilitatea de a determine daca a fost publicat un nou CRL).

6.2.1. Extensiile acceptate in intrarile din CRL

Rolul si semnificatia extensiilor este aceleasi ca in cazul extensiilor de certificat. Extensiile dintr-o intrare CRL (*crlEntryExtensions*) acceptate de AlfaTrust Certification contin urmatoarele campuri:

- ***ReasonCode***: codul motivului revocarii certificatului. Acest camp nu este critic si permite determinarea motivului revocarii unui certificat. Sunt permise urmatoarele motive de revocare:
  - ✓ *unspecified, certificateHold* – nespecificat;
  - ✓ *keyCompromise* – compromiterea cheii;
  - ✓ *cACompromise* – compromiterea cheii Autoritatii de Certificare;
  - ✓ *affiliationChanged* – modificarea datelor Abonatului;
  - ✓ *superseded* – innoirea certificatului;
  - ✓ *cessationOfOperation* – sistarea folosirii certificatului;
  - ✓ *removeFromCRL* – eliminarea certificatului din CRL.

6.3. Profilul raspunsului de confirmare OCSP

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

Serviciul OCSP este oferit de AlfaTrust Certification in numele tuturor Autoritatilor de Certificare afiliate. Serverul OCSP, care emite confirmari ale starii certificatelor, foloseste o pereche speciala de chei, generata exclusiv pentru acest scop.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

Certificatul serverului OCSP trebuie sa contina extensia *ExtKeyUsage*, descrisa in RFC 3280. Aceasta extensie trebuie declarata ca fiind non-critica si semnifica faptul ca o Autoritate de Certificare care emite certificatul pentru serverului OCSP confirma prin semnatura sa delegarea autorizarii de a emite confirmari ale starii certificatelor (apartinand utilizatorilor acestei autoritati).

De asemenea, certificatul serverului OCSP contine extensia *OCSPNoCheck*, descrisa de RFC 2560. Aceasta extensie trebuie declarata ca fiind non-critica si semnifica faptul ca un client de OCSP care primeste un raspuns semnat cu cheia privata asociata acestui certificat va putea avea incredere in starea certificatului serverului OCSP, nefiind necesara verificarea starii de revocare a acestuia.

Entitatea care primeste o confirmare emisa de serverul OCSP trebuie sa suporte formatul standard de raspuns avand 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. Numarul versiunii

Serverul OCSP care opereaza in cadrul AlfaTrust Certification emite confirmari ale starii certificatelor in conformitate cu RFC 2560. Singura valoare permisa a numarului versiunii este 0 (este echivalentul versiunii v1).

6.3.2. Informatiile despre starea certificatului

Informatiile despre starea certificatului se afla in campul *certStatus* al structurii ***SingleResponse***. Acesta poate avea una dintre cele trei valori principale:

- ✓ **GOOD** – indica faptul ca certificatul este in stare valida
- ✓ **REVOKED** – indica faptul ca certificatul a fost emis si a fost revocat
- ✓ **UNKNOWN** – indica faptul ca nu exista suficiente informatii pentru determinarea starii certificatului respectiv.

6.3.3. Extensiile standard acceptate

In concordanta cu RFC 2560, serverul OCSP al AlfaTrust Certification accepta urmatoarea extensie:

- ✓ ***Nonce*** – leaga o cerere de un raspuns pentru a preveni atacurile prin reluare. Nonce este inclus in *requestExtensions* al ***OCSPRequest*** si repetat in campul *responseExtensions* al ***OCSPResponse***.

7. Managementul DPSI

Fiecare versiune a DPSI este in vigoare pana in momentul aprobarii si publicarii noii sale versiuni. O noua versiune este dezvoltata de catre AlfaTrust Certification si publicata pentru comentarii cu mentiunea spre aprobare (daca este cazul). Dupa primirea si includerea comentariilor, DPSI intra in procedura de aprobare interna. Responsabil de aprobarea formei finale a DPSI este un comitet format din directorul general si

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro

managerii departamentelor din AlfaTrust Certification. Responsabil pentru intretinerea DPSI este managerul departamentului care asigura furnizarea serviciilor de certificare. Dupa terminarea procedurii de aprobare, noua versiune a DPSI este transmisa Organismului de Supraveghere si apoi, in teremen de 10 zile, este publicata si marcata ca fiind in starea valida.

Modificarea DPSIpoate fi rezultatul depistarii unor erori, actualizarii sale sau a sugestiilor primite din partea entitatilor interesate. Propunerile de modificare pot fi trimise prin posta sau e-mail pe adresa AlfaTrust Certification S.A. Propunerile de modificare trebuie sa descrie modificarile necesare, motivele acestor modificari si sa ofere mijloace de contact ale persoanei care solicita modificarea.

Modificarile introduse pot fi in general impartite in doua categorii: una care nu necesita consultarea utilizatorilor si entitatilor partenere si una care cere (de obicei in avans) consultarea acestora. Prima categorie include modificari de urgenta sau modificari neesentiale.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97,
office@alfasign.ro