certSIGN

Şoseua Olteniţei, 107A
Sector 4, 041303,
Bucureşti, România

Tel.: (+4021) 311 99 04
Fax: (+4021) 311 99 05
E-mail: office@certsign.ro
Web: www.certsign.ro

Codul de Practici şi Proceduri

certSIGN

Versiunea 1.5

Data: October, 2009

certSIGN

Şoseua Olteniţei, 107A
Sector 4, 041303,
Bucureşti, România

Tel.: (+4021) 311 99 04
Fax: (+4021) 311 99 05
E-mail: office@certsign.ro
Web: www.certsign.ro

certSIGN

Şoseua Olteniţei, 107A
Sector 4, 041303,
Bucureşti, România

Tel.: (+4021) 311 99 04
Fax: (+4021) 311 99 05
E-mail: office@certsign.ro
Web: www.certsign.ro

Istoria documentului

Versiune	Data	Motiv	Persoana care a facut modificarea
1.0	Aprilie 2006	Publicarea primei versiuni	Manager Servicii Electronice
1.1	Iulie 2006	Termen de 1 an pt revizuirea clasificarii	Manager Servicii Electronice
1.2	Octombrie 2008	S-a introdus numele persoanei responsabile cu administrarea CPS-ului ca si adresa de contact a acesteia.	Manager Servicii Electronice
		S-au introdus detalii referitoare la modul de protejare si backup al cheilor private de criptare ale abonatilor.	Manager Servicii Electronice
		S-a clarificat pozitia firmei certSIGN ca furnizor de servicii de certificare fata de utilizarea marcilor inregistrate in certificatele digitale.	Manager Servicii Electronice
		S-a specificat ca, pentru moment certSIGN nu foloseste serviciilor unor RA-uri externe.	Manager Servicii Electronice
		S-a specificat ca certSIGN nu ofera servicii de suspendare a certificatelor.	Manager Servicii Electronice
		S-a specificat ca mesajele de eroare ca raspuns la cererile de verificare online a starii certificatelor (prin OCSP) nu sunt semnate digital.	Manager Servicii Electronice
		S-a specificat ca certSIGN nu are implementate procese de management al ciclului de viata al tokenurilor/smartcardurilor.	Manager Servicii Electronice
		S-au dat detalii suplimentare despre site-ul de disaster recovery.	Manager Servicii Electronice
		S-a precizat ca certSIGN nu ofera servicii de key management pt abonati.	Manager Servicii Electronice
		S-a precizat ca certSIGN nu ofera servicii de schimbare a cheii unui certificate.	Manager Servicii Electronice
1.3	Februarie 2009	S-a detaliat procedura de verificare de catre RA a controlului exercitat de solicitantul certificatelor de server asupra domeniului	Manager Servicii Electronice
		S-a detaliat procedura de verificare de catre RA a controlului exercitat de abonat asupra contului de mail declarat in cererea de certificat	Manager Servicii Electronice
1.4	Iulie 2009	S-a modificat adresa firmei	Manager Servicii Electronice
1.5	Octombrie 2009	S-au introdus conditiile pentru CA-urile subordinate operate de terti	Manager Servicii Electronice

Acest document a fost creat si este proprietatea:

Proprietar	Autor	Data crearii
Manager Servicii Electronice	Manager Servicii Electronice	27 Ianuarie 2006

Lista de Distributie

Destinatar	Data distribuirii
Public-Internet	2 Noiembrie 2009

Acest document a fost aprobat de

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Aprilie 2006
1.1	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Iulie 2006
1.2	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	August 2008
1.3	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de incredere	Februarie 2009
1.4	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de incredere	Iulie 2009
1.5	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de incredere	Octombrie 2009

Cuprins

1 Introducere

Codul de Practici şi Proceduri al certSIGN – (denumit în continuare **Codul de Practici şi Proceduri** sau **CPP**) descrie procesul de certificare a cheilor publice şi aria de aplicabilitate a certificatelor care rezultă din acest proces de certificare. Codul de Practici şi Proceduri prezintă importanță în mod special pentru Abonați şi Entitățile Partenere. **Codul de Practici şi Proceduri** descrie regulile generale ale procesului de certificare, stipulate în **Politica de certificare certSIGN** (denumită în continuare **Politica de certificare** sau **CP**). **Politica de certificare** descrie nivelul de încredere ce poate fi acordat unui anumit tip de certificat emis de **Furnizorul de Servicii de certificare certSIGN** (denumit în continuare **certSIGN**). **Codul de Practici şi Proceduri** descrie modalitatea prin care certSIGN asigură nivelul de încredere garantat de politică.

Codul de Practici şi Proceduri descrie patru politici de certificare aplicate de către certSIGN în vederea emiterii de certificate pentru autorități şi utilizatorii finali. Aceste politici reprezintă patru nivele diferite de credibilitate (**Clasa 1, Clasa 2, Clasa 3, Clasa 4**) corespunzătoare certificatelor de chei publice. Ariile de aplicabilitate ale certificatelor emise în conformitate cu aceste politici pot fi aceleaşi. Cu toate acestea, responsabilitățile (inclusiv din punct de vedere legal) ale Autorității de certificare şi utilizatorilor de certificate sunt diferite. Structura şi conținutul Codului de Practici şi Proceduri sunt în conformitate cu recomandările RFC 3647. Codul de Practici şi Proceduri presupune faptul că cititorul este familiar cu noțiunile privind certificatele, semnatura electronica şi Infrastructurile de Chei Publice (PKI).

Există mai multe documente auxiliare care au legătură cu Codul de Practici şi Proceduri. Acestea sunt folosite în cadrul Autorităților de certificare certSIGN pentru a reglementa modul de funcționare al acestora. Aceste documente au însă un statut diferit şi nu sunt disponibile public datorită importanței informațiilor pe care le conțin pentru securitatea sistemului.

Informații adiționale despre Codul de Practici si Proceduri se pot obține prin poşta electronica de la Managerul Serviciilor Electronice la adresa: office@certsign.ro.

1.1 Privire de ansamblu asupra procesului de certificare

Codul de Practici şi Proceduri este specificația ce stă la baza funcționarii **certSIGN** şi a **Autorităților de certificare**, **a Autorității de Înregistrare**, **Abonaților şi a Entităților Partenere** asociate acesteia. De asemenea, acest document descrie regulile de prestare a serviciilor de certificare cum ar fi înregistrarea Abonaților, certificarea cheilor publice, înnoirea cheilor şi a certificatelor şi revocarea certificatelor.

Arhitectura Infrastructurii de Chei Publice (PKI) a **certSIGN** este împărțită pe doua nivele (vezi Figura 1.1). Nivelul 1 conține **certSIGN ROOT CA**. Autoritățile de certificare de pe Nivelul 2 sunt direct semnate de către **certSIGN ROOT CA**. **certSIGN ROOT CA** operează numai în mod off-line. În cazul compromiterii **certSIGN CA 2,3, sau 4**, **certSIGN ROOT CA** va fi folosită pentru a revoca certificatele acestora şi pentru a emite noi certificate.

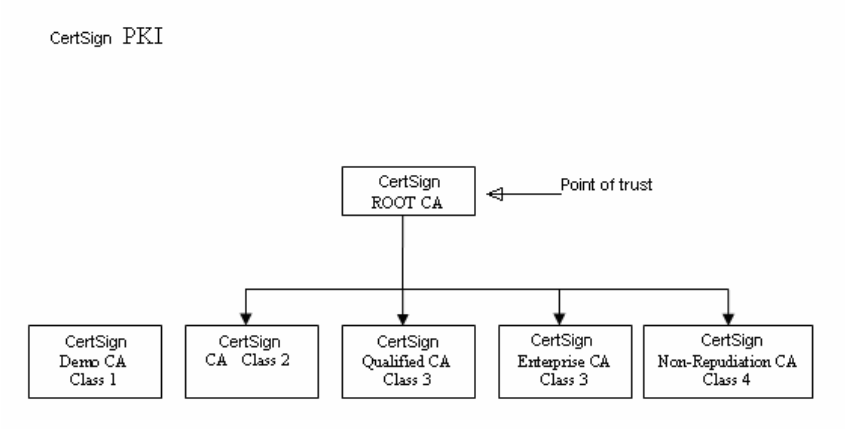

Figura 1.1. Autoritățile de emitere certificate ce operează în cadrul certSIGN

Din punct de vedere ierarhic, există patru Autorități de certificare, imediat subordonate **certSIGN ROOT CA**:

- certSIGN CA Class 2
- certSIGN Qualified CA Class 3
- certSIGN Entreprise CA Class 3
- certSIGN Non-Repudiation CA Class 4

toate emițând certificate având nivele de credibilitate diferite.

certSIGN CA Class 1 este o autoritate autosemnata care emite doar certificate demo.

Momentan, certSIGN nu are nici un acord reciproc de certificare cu o altă autoritate de emitere de certificate. Dacă această situaţie se va schimba, utilizatorii vor fi informaţi despre acest lucru prin publicarea unei noi versiuni a Politicii de certificare (CP) şi a Codului de Practici şi Proceduri (CPP).

Certificatele emise de certSIGN conţin identificatorii politicii de certificare, permiţând astfel Entităţilor Partenere să stabilească dacă certificatul verificat a fost folosit în conformitate cu scopul declarat al acestuia. Scopul declarat este specificat pe baza valorilor din câmpul *PolicyInformation* al extensiei *certificatesPolicies* (vezi Capitolul 7.1.1.2) din cadrul fiecărui certificat emis de certSIGN.

Tipurile de certificate emise de către Autorităţile de certificare sunt descrise în Tabelul 1.1.

Clasa	Tipul	Subtipul
Clasa 1 (Demo)	certificat demonstrativ simplu	
	certificat demonstrativ pentru semnarea de cod	
	certificat demonstrativ pentru servere Web	
	certificat demonstrativ pentru gateway-uri VPN	
	certificat demonstrativ pentru servere CA	
	certificat demonstrativ pentru servere TSA	
	certificat demonstrativ pentru servere de validare (OCSP)	
Clasa 2	certificat simplu	certificat simplu pentru autentificare şi semnare ▪ fără DSCS şi cheie generată de Abonat ▪ cu DSCS şi cheie generată de Abonat ▪ cu DSCS şi cheie generată de certSIGN certificat simplu pentru criptare ▪ fără DSCS şi cheie generată de Abonat ▪ cu DSCS şi cheie generată de Abonat ▪ cu DSCS şi cheie generată de certSIGN
Clasa 3	certificat calificat	certificat calificat ▪ cu DSCS şi cheie generată de Abonat ▪ cu DSCS şi cheie generată de certSIGN
	certificat de criptare de încredere	certificat de criptare de încredere ▪ cu DSCS şi cheie generată de Abonat ▪ cu DSCS şi cheie generată de certSIGN
	certificat pentru semnarea de cod	
	certificat pentru servere Web	
	certificat pentru gateway-uri VPN	
Clasa 4	certificat pentru servere CA	
	certificat pentru servere TSA	
	certificat pentru servere de validare (OCSP)	

Tabelul 1.1. Tipuri de certificate

1.2 Identificarea CPP

Denumirea acestui document este: Codul de Practici şi Proceduri al certSIGN. Documentul este disponibil:

- sub formă electronica în Depozit la adresa http://www.certsign.ro/repository sau pe baza unei cereri trimisă pe adresa office@certsign.ro;
- sub formă tipărită, pe baza unei cereri trimisă pe adresa certSIGN (vezi Capitolul 1.5).

1.3 Părțile din cadrul CPP

Codul de Practici şi Proceduri reglementează cele mai importante relații dintre entități aparținând certSIGN, echipele de consultanți (inclusiv auditorii) şi clienții (utilizatorii serviciilor furnizate) acesteia:

- Autoritățile de certificare:
- certSIGN ROOT CA,
- certSIGN Demo CA Class 1,
- certSIGN CA Class 2,
- certSIGN Qualified CA Class 3,
- certSIGN Entreprise CA Class 3,
- certSIGN Non-Repudiation CA Class 4,
- Autoritatea de Înregistrare
- Depozitul,
- Serverul de verificare on-line a stării certificatelor (OCSP),
- Abonații,
- Entitățile Partenere.

certSIGN oferă servicii de certificare pentru orice *persoană fizică* sau *juridică* care este de acord cu prevederile prezentului Cod de Practici şi Proceduri. Scopul acestor practici (ce includ procedurile de generare a *cheilor*, procedurile de emitere a *certificatelor* şi *securitatea sistemului informaţional*) este acela de a garanta utilizatorilor serviciilor certSIGN că nivelele de credibilitate declarate ale certificatelor emise corespund practicilor Autorităților de certificare.

1.3.1 Autoritățile de Certificare

Autoritatea de Certificare **certSIGN ROOT CA** este o Autoritate de Certificare Primară pentru domeniul certSIGN. Toate celelalte Autorități de Certificare din cadrul acestui domeniu sunt subordonate certSIGN ROOT CA (vezi Figura 1.3).

În prezent există patru Autorități de Certificare subordonate direct lui certSIGN ROOT CA: **certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3** , **certSIGN Non-Repudiation CA Class 4** si una autosemnata, **certSIGN Demo CA Class 1,**

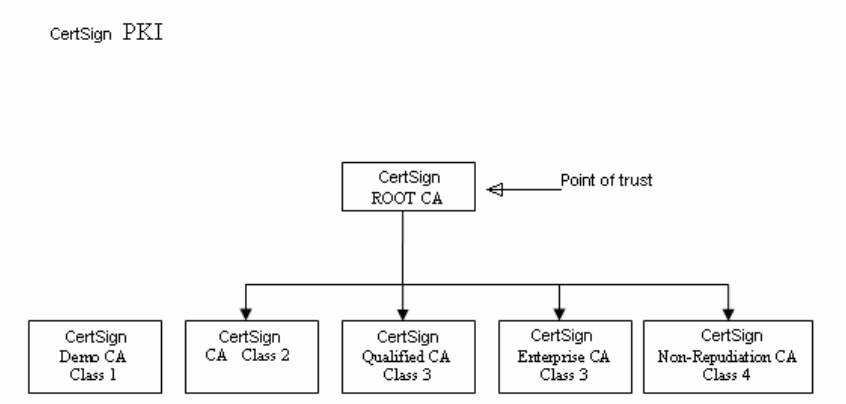

Figura 1.3. Structura domeniului de certificare certSIGN

Autoritatea de Certificare Primară, **certSIGN ROOT CA**, poate înregistra şi emite certificate numai Autorităților de certificare şi autorităților ce emit confirmări electronice de ne-repudiere ce aparțin domeniului certSIGN. Înainte de a începe activitatea, fiecare autoritate de certificare subordonată trebuie să trimită o cerere către Autoritatea de Certificare Principală, **certSIGN ROOT CA** pentru înregistrare şi emitere de certificat de cheie publică (a se vedea şi procedurile descrise în capitolul 6.1 din *prezentul cod de practici şi proceduri*). Autoritatea **certSIGN ROOT CA** funcționează pe baza unui certificat *autosemnat*, emis de ea însăşi. Într-un astfel de

certificat, extensia **certificatePolicies** lipseşte (vezi Capitolul 7.1.1), ceea ce semnifică faptul că nu există limitări ale setului de **căi de certificare** la care certificatul certSIGN ROOT CA poate fi ataşat.

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

Autoritatea de Certificare **certSIGN ROOT CA** furnizează servicii de certificare pentru:

- sine (emite şi reînnoieşte certificate proprii),
- Autoritățile de Certificare înregistrate în domeniul de certificare certSIGN,
- entități ce furnizează servicii de verificare on-line a stării certificatelor şi alte entităților ce oferă servicii de ne-repudiere (de exemplu, servicii de marcare temporala).

Autoritățile de certificare subordonate **certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3**, **certSIGN Non-Repudiation CA Class 4 si autoritatea auosemnata certSIGN Demo CA Class 1,** emit certificate către Abonați, conform politicilor având identificatorii din Tabelul 1.3.

Autoritatea de Certificare	Politica de certificare
certSIGN Demo CA Class 1	**{certSIGN}* id-policy(1) id-cp(1)id-Class-1(1)**
certSIGN CA Class 2	**{certSIGN} id-policy(1) id-cp(1)id-Class-2(2)**
certSIGN Qualified CA Class 3	**{certSIGN} id-policy(1) id-cp(1)id-Class-3(3) si itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1)**
certSIGN Entreprise CA Class 3	**{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)**
certSIGN Non-Repudiation CA Class 4	**{certSIGN} id-policy(1) id-cp(1)id-Class-4(4)**

Tabelul 1.3. Numele Autorităților de Certificare şi politicile de certificare corespunzătoare

Autoritățile de Certificare subordonate sunt configurate pentru a emite certificate către:

- utilizatori care vor să-şi asigure securitatea şi credibilitatea poştei electronice şi a altor servicii (de exemplu, comerț electronic, biblioteci de informații şi software) prin intermediul certificatelor,

* {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (25017)

- entități care oferă servicii de ne-repudiere (autorități de marcare temporala),
- furnizori de servicii din domeniul telecomunicațiilor mobile,
- dispozitive de rețea care realizează conexiuni criptate peste VPN,
- dispozitive hardware (fizice şi logice) deținute de persoane particulare sau juridice, în vederea oferirii de servicii pe bază de certificate de chei publice cum ar fi serviciul de verificare on-line a stării certificatelor (OCSP),
- alte Autorități de Certificare.

Orice entitate externa care doreste incheierea unui contract pentru operarea unui CA subordonat certSIGN Non-Repudiation CA Class 4 va incheia cu certSIGN un contract prin care se obliga sa respecte versiunile curente ale CP si ale CPS si sa se supuna unui audit pentru verificarea conformitatii cu standardul WebTrust for CA.

1.3.2 Autoritatea de Înregistrare

Autoritatea de Înregistrare primeşte, verifică şi aprobă sau respinge cererile de înregistrare şi emitere de certificate, de reînnoire sau revocare a certificatelor. Verificarea cererilor are ca scop autentificarea (pe baza documentelor incluse în cereri) atât a solicitantului cât şi a datelor menționate în cerere. Autoritatea de Înregistrare poate trimite cereri către Autoritatea de Certificare corespunzătoare – pentru anularea cererii de înregistrare a unui Abonat şi pentru retragerea certificatului acestuia.

Nivelul de precizie al procesului de determinare a identității clientului este dat de nevoile Abonatului şi este impus de nivelul certificatului pe care îl solicită Abonatul (vezi Capitolul 3). În cazul celei mai simple identificări, Autoritatea de Înregistrare verifică doar corectitudinea adresei de e-mail trimisă. Cea mai precisă identificare presupune prezența în persoană a solicitantului la Autoritatea de Înregistrare şi furnizarea de dovezi cu privire la identitatea sa. Identificarea poate fi realizată fie automat**,** fie manual de către un operator al Autorității de Înregistrare.

Autoritatea de Înregistrare funcționează pe baza autorizației obținute de la o Autoritate de certificare corespunzătoare aparținând domeniului certSIGN si nu poate opera decât în cadrul firmei certSIGN, în prezent nefiind admise Autorități de Înregistrare externe.

1.3.3 Depozitul

Vezi 2.6 Depozitul şi publicarea informațiilor

1.3.4 Utilizatorii finali

Utilizatorii finali sunt Abonații şi entitățile partenere. Un Abonat este o entitate al cărei identificator este plasat în câmpul *Subject* al unui certificat şi care nu emite certificate altor entități. O Entitate Parteneră este o entitate care foloseşte certificatul unui Abonat pentru a verifica semnatura electronica a acestuia sau pentru a asigura confidențialitatea informațiilor transmise.

Abonații

Orice persoană fizică sau juridică, precum şi dispozitivele hardware pe care acestea le dețin pot fi Abonați ai certSIGN – CA, cu condiția să se încadreze în termenii din definiția Abonatului (vezi Capitolul 1.3.4). În particular, operatorii Autorității de Înregistrare, ceilalți angajați certSIGN şi echipamentele indispensabile pentru asigurarea securității infrastructurii certSIGN (firewall-uri, routere, servere de autentificare) reprezintă, de asemenea, Abonați.

Organizațiile care doresc să obțină certificate emise de certSIGN pentru angajații lor, pot să o facă prin intermediul reprezentanților lor, pe când Abonații individuali trebuie să ceară personal un certificat.

certSIGN emite certificate de tipuri diferite şi de nivele de credibilitate diferite. Abonații trebuie să decidă ce tip de certificat este cel mai potrivit pentru nevoile lor (vezi Capitolul 1.4).

Entitățile partenere

Entitate Parteneră, ce utilizează serviciile certSIGN, poate fi orice entitate care ia decizii bazându-se pe corectitudinea conexiunii dintre identitatea unui Abonat şi cheia sa publică (conexiune confirmată de una din Autoritățile de certificare subordonate certSIGN ROOT CA).

O Entitate Parteneră este responsabilă pentru modul în care verifică starea curentă a certificatului unui Abonat. O astfel de decizie trebuie luată de fiecare dată când o Entitate Parteneră doreşte să utilizeze un certificat pentru a verifica o semnatura electronica, pentru a verifica identitatea sursei sau autorul unui mesaj, sau pentru a crea un canal de comunicație secret cu proprietarul certificatului. O Entitate Parteneră trebuie să utilizeze informațiile dintr-un certificat (de exemplu, identificatorii şi calificatorii politicii de certificare) pentru a decide dacă un certificat a fost folosit în conformitate cu scopul declarat.

1.4 Aria de aplicabilitate a certificatelor

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

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

Certificatele emise de certSIGN pot fi folosite pentru a procesa şi asigura securitatea informațiilor (inclusiv autentificarea), având nivele diferite de credibilitate. Nivelul de credibilitate al informației şi vulnerabilitatea acesteia trebuie evaluate de către Abonat. În Politica de certificare şi prezentul Cod de Practici şi Proceduri sunt definite patru nivele de sensibilitate: Clasa 1 (nivelul de test), Clasa 2 (nivelul de bază), Clasa 3 (nivelul intermediar), Clasa 4 (nivelul ridicat). Aceste nivele corespund celor patru nivele de credibilitate ale certificatelor (vezi Tabelul 1.4).

Nivelul de sensibilitate al informației	Numele politicii de certificare	Aria de aplicabilitate
Clasa 1 (de test)	certSIGN Class 1	Cel mai scăzut nivel de credibilitate al identității unei entități. Certificatele de Clasa 1 se recomandă a se folosi pentru a testa compatibilitatea serviciilor certSIGN cu cele oferite de alți furnizori de servicii PKI şi pentru a testa funcționalitatea certificatelor în cadrul aplicațiilor testate. De asemenea, aceste certificate pot fi folosite în alte scopuri atâta timp cât asigurarea credibilității mesajelor trimise sau primite nu este importantă.
Clasa 2 (de bază)	certSIGN Class 2	Acest nivel oferă o securitate de bază pentru informații în medii cu grad scăzut de risc (risc fără consecințe majore). Dintre acestea, menționăm accesul la informații private acolo unde probabilitatea de apariție a unui

		acces neautorizat nu este foarte mare. Aceste certificate pot fi folosite pentru a autentifica şi controla integritatea informației care a fost semnată şi pentru a asigura confidențialitatea informației, mai ales în cazul poştei electronice.
Clasa 3 (intermediar)	certSIGN Class 3	Acest nivel se recomandă pentru asigurarea securității informației în medii unde există riscul apariției de breşe de securitate iar consecințele acestor breşe sunt moderate. Certificatele pot fi folosite pentru protecția tranzacțiilor financiare sau a tranzacțiilor în care există şanse de apariție a fraudelor. De asemenea, aceste certificate pot fi folosite şi pentru crearea de semnaturi electronice extinse.
Clasa 4 (ridicat)	certSIGN Class 4	Acest nivel corespunde mediilor în care şansele compromiterii datelor sunt foarte mari şi în care consecințele unui incident de securitate sunt foarte grave. Aceste certificate pot fi folosite pentru protecția tranzacțiilor de valoare nelimitată (dacă nu se specifică altceva în certificat), a tranzacțiilor în care există mari şanse de apariție a fraudelor.

Tabel 1.4. Nivelul de sensibilitate al informației şi denumirea politicii

Entitatea parteneră este responsabilă pentru stabilirea nivelului de credibilitate necesar pentru un certificat folosit într-un anume scop. Luând în considerare factorii de risc semnificativi, entitatea parteneră trebuie să stabilească ce tip de certificat emis de certSIGN se potriveşte cerințelor formulate. Abonații trebuie să cunoască cerințele entității partenere (de exemplu, aceste cerințe pot fi publicate sub forma unei politici de semnatura sau politică de securitate informatică) şi apoi să solicite certSIGN emiterea de certificate corespunzătoare acestor cerințe.

1.4.1 Aria de aplicabilitate recomandată

certSIGN emite opt tipuri de bază de certificate având arii diferite de aplicabilitate. Aceste sunt:

1. **certificate pentru Autoritățile de Certificare** – folosirea lor nu este restricționată la aria definită; aria de aplicabilitate poate fi dată de extensia din certificate ce stabileşte modul în care poate fi folosită cheia privată (vezi câmpul **keyUsage**, Capitolul 7), sau de rolul acesteia (de exemplu, Abonat, Autoritate de Certificare sau altă autoritate care furnizează servicii PKI); acest tip conține de asemenea şi certificatele operaționale ale Autorităților de Certificare;
2. **certificate pentru confirmarea autenticității serverelor** – sunt folosite de serviciile care operează pe baza protocoalelor SSL/TLS/WTLS;
3. **certificate simple de semnare şi autentificare** – permit semnarea emailurilor şi fişierelor, sau autentificarea unui abonat (de exemplu prin protocolul SSL);

4. **certificate calificate** – permit semnarea documentelor cu valoare juridică;
5. **certificate pentru confirmarea stării unui certificat** – sunt emise pentru serverele care funcționează conform protocolului OCSP şi care furnizează informații despre starea certificatelor;
6. **certificate pentru Autorități de Marcare Temporala** – sunt emise serverelor care, ca răspuns la cererea unui Abonat, emit mărci temporale prin care asociază unor date (documente, mesaje, semnaturi electronice etc.) un moment de timp pe baza căruia se poate determina secvențialitatea în timp a datelor;
7. **certificate de criptare** – folosite pentru asigurarea securității e-mail-urilor, fişierelor şi directoarelor;
8. **certificate pentru securizarea codului** – folosite de programatori pentru a proteja software-ul împotriva falsificării.

Certificatele emise în concordanță cu una dintre cele patru politici de certificare pot fi folosite în aplicații ce satisfac cel puțin următoarele condiții:

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

Lista aplicațiilor recomandate (de către certSIGN) este publicata pe site la adresa: http://www.certsign.ro/.

Aplicațiile sunt incluse în lista aplicațiilor recomandate pe baza unor declarații scrise ale producătorilor şi/sau pe baza testelor făcute de certSIGN. certSIGN permite fiecărui Abonat să-şi genereze singur cheile criptografice folosite în procesul de certificare prin intermediul dispozitivelor recomandate. Autoritatea de Certificare poate de asemenea să genereze cheile pe un dispozitiv criptografic şi apoi să livreze Abonatului dispozitivul împreună cu cheile. În acest

caz, certSIGN foloseşte dispozitive criptografice ce satisfac cel puțin cerințele standardului FIPS PUB 140-2.

1.4.2 Aplicații interzise

Este interzisă folosirea certificatelor certSIGN pentru alte scopuri decât cele declarate şi în aplicații care nu îndeplinesc condițiile minime specificate în 1.4.1.

1.5 Adresa de contact

Adresa: Sos. Oltenitei nr. 107A, C1, parter, Cod poştal 041303

E-mail: office@certsign.ro

Telefon: 021 311 99 04

Fax: 021 311 99 05

Informații adiționale despre Codul de Practici si Proceduri se pot obține prin poşta electronica de la Manager Servicii Electronice la adresa: office@certsign.ro.

2 Prevederi generale

Acest capitol descrie obligaţiile / garanţiile şi responsabilităţile Furnizorului de Servicii de certificare certSIGN, Autorităţii de Înregistrare, Abonaţilor şi utilizatorilor de certificate (entităţi partenere). Obligaţiile şi responsabilităţile sunt guvernate de acorduri mutuale stabilite între părţile menţionate mai sus (vezi Figura. 2).

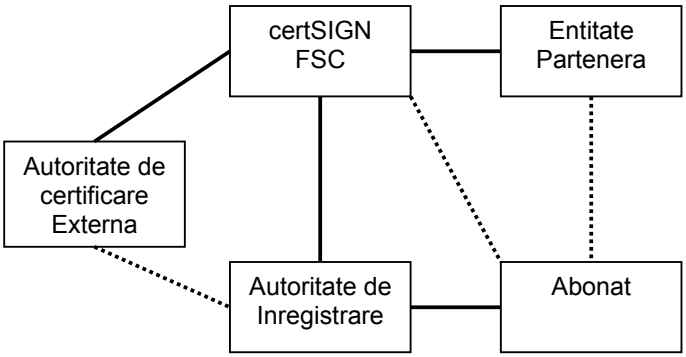

Figura 2 Acordul între părţi

Contractele încheiate de certSIGN cu Entităţile Partenere şi Abonaţii descriu tipurile de servicii furnizate de certSIGN, obligaţiile mutuale şi responsabilităţile acestora.

Autoritatea de Certificare certSIGN poate înregistra şi emite un certificat oricărei entităţi externe care joacă rolul de Autoritate de Certificare subordonată, cu condiţia ca înregistrarea şi emiterea certificatului să se facă pe baza unui contract încheiat între cele două părţi.

Codul de Practici şi Proceduri şi Politica de certificare sunt parte integrantă a contractelor încheiate între certSIGN şi Abonaţi, Entităţile Partenere, sau alte entităţi care furnizează servicii specifice infrastructurilor de chei publice, cum ar fi marcarea temporala, verificarea stării certificatelor etc.

Contractele încheiate între o Entitate Parteneră şi un Abonat vor respecta întocmai prevederile prezentului Cod de Practici şi Proceduri, prevederile acestuia prevalând în caz de dubiu sau neconcordanţă.

2.1 Obligații

2.1.1 Obligațiile certSIGN

certSIGN garantează că:

- activitatea sa comercială se bazează pe dispozitive fiabile şi aplicații software de încredere,
- activitatea şi serviciile sale sunt în concordanță cu prevederile legale, nu încalcă drepturile de autor şi nici drepturile terțelor părți,
- serviciile sale sunt în concordanță cu normele larg acceptate:
  - servicii de certificare – conform X.509, PKCS#10, PKCS#7, PKCS#12,
  - servicii de marcă temporala – conform standardului RFC 3161,
  - verificarea stării certificatelor (OCSP) – conform standardului RFC 2560.
- respectă şi impune procedurile descrise în prezentul Cod de Practici şi Proceduri, în special cele cu privire la:
  - verificarea informațiilor referitoare la identitatea Abonatului căruia îi este emis un certificat aparținând domeniului certSIGN; procedurile de verificare a identității Abonatului depind de informațiile incluse în certificat şi variază în funcție de taxele de certificare, natura şi identitatea Abonatului şi aria de aplicabilitate a certificatului (vezi Capitolele 3 şi 4),
  - certificatele care sunt revocate, în cazul existenței supoziției sau siguranței că certificatul conține date care nu mai sunt de actualitate, sau că cheia privată corespunzătoare certificatului a fost compromisă (dezvăluită, pierdută etc.),
  - informarea Abonatului şi a altor entități interesate în cazurile în care Abonatul este subiectul unui certificat emis, revocat sau suspendat,
  - publicarea listelor cu certificatele revocate sau suspendate în locurile stabilite prin prezentul Cod,

- generarea şi folosirea cheilor private numai în scopurile declarate în prezentul Cod; protecţia cheilor astfel încât să nu se permită folosirea lor în alte scopuri decât cele admise,
- personalizarea şi emiterea dispozitivelor criptografice, *pe care sunt stocate certificatele şi perechea de chei* (când cheia este generată de o Autoritate de Certificare),
- publicarea informaţiilor necesare pentru recepţia corectă, managementul şi revocarea certificatelor,

- nu are cunoştinţă că certificatele emise conţin informaţii false, ştiute sau provenind de la persoanele care aprobă cererile pentru emiterea de certificate sau care emit certificate
- certificatele emise nu conţin nici o informaţie falsificată, ştiută sau provenind de la persoanele ce aprobă cererile pentru emiterea de certificate sau care emit certificate,
- certificatele emise nu conţin nici o greşeală care să rezulte din neglijenţă sau din violarea procedurilor de către persoanele ce aprobă cererile pentru emiterea de certificate sau care emit certificate,
- numele distincte ale Abonaţilor, care apar în certificate, sunt unice pentru domeniul certSIGN,
- asigură protecţia datelor cu caracter personal în concordanţă cu Legea nr. 677/2001 privind protecţia datelor cu caracter personal si cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- dacă o pereche de chei este generată cu autorizarea Abonatului, perechea de chei este livrată în mod confidenţial Abonatului şi imediat după livrarea acesteia, este ştearsă de pe suportul folosit pentru livrare, cu excepţia cazului în care Abonatul cere arhivarea perechii de chei.

certSIGN se angajează:

- să înregistreze şi să emită certificate numai pentru Autorităţi de Certificare a căror politică de certificare şi cod de practici şi proceduri au fost aprobate de către certSIGN; certSIGN poate solicita ca cel puţin una din cele patru politici de certificare (specificate în Tabelul 1.3 şi Capitolul 7.1.1.2) să fie aplicate de către Autoritatea de Certificare înregistrată,
- să încheie contracte cu Abonaţii, Entităţile Partenere (daca este cazul) si Autorităţile de Certificare; serviciile de certificare sunt furnizate numai pe baza contractelor şi întotdeauna la solicitarea unui Abonat, Entităţi partenere, Autorităţi de Certificare,
- să creeze şi să administreze o listă de aplicaţii software şi dispozitive recomandate a se folosi pentru generarea de perechi de chei asimetrice,
- să creeze şi să administreze o listă de aplicaţii recomandate care îndeplinesc cerinţele din Capitolul 1.4.1,
- să efectueze auditurile planificate în cadrul Autorităţilor de Certificare şi Autorităţii de Înregistrare care aparţin domeniului certSIGN;
- să solicite unor auditori independenţi efectuarea unor evaluări pentru domeniul certSIGN, să pună la dispoziţia acestora documentele şi informaţiile necesare şi să urmeze recomandările auditorilor.

2.1.2 Obligaţiile Autorităţii de Înregistrare

Autoritatea de Înregistrare operând în domeniul certSIGN garantează că:

- activitatea sa comercială se bazează pe dispozitive fiabile şi aplicaţii software recomandate de certSIGN,
- activitatea şi serviciile sale sunt în concordanţă cu legea, nu încalcă drepturile de autor şi nici drepturile terţelor părţi,
- datele de identificare ale Abonaţilor introduse în baza de date a certSIGN corespund datelor puse la dispozitie de Abonat şi aceste informaţii vor fi actualizate imediat ce a luat la cunostinta de modificarile intervenite,

- informaţia despre Abonat validată şi trimisă ulterior către Autoritatea de Certificare pentru a fi inclusă în certificat, este corectă,
- nu contribuie în mod intenţionat sau neintenţionat la apariţia de greşeli sau inexactităţi ale informaţiilor conţinute în certificat,
- serviciile prestate sunt în concordanţă cu normele larg acceptate (de jure şi de facto): X.509, PKCS#10, PKCS#7, PKCS#12,
- serviciile prestate sunt furnizate pe baza unor proceduri conforme cu recomandările prezentului Cod de Practici şi Proceduri; în special cele cu privire la:
  - procedurile de verificare a identităţii Abonaţilor,
  - procedura pentru demonstrarea posesiei cheii private, asociată cu cheia publică pentru care se solicită certificarea,
  - procedurile de recepţie, procesare şi confirmare sau respingere a cererilor clienţilor pentru emiterea, reînnoirea □i revocarea,
  - procedurile de transmitere a cererilor unei Autorităţi de Certificare, pe baza unei cereri acceptate a unui Abonat, pentru emiterea, reînnoirea sau revocarea,;
  - procedurile de arhivare a cererilor şi informaţiilor primite de la Abonaţi, a deciziilor luate şi a informaţiilor trimise Autorităţilor de Certificare,
  - procedurile de generare a cheilor pentru Abonaţi, cu condiţia ca contractul încheiat cu Autoritatea de Certificare şi cu Abonatul să permită acest lucru; cheile nu pot fi stocate de către Autoritatea de Înregistrare decât dacă contractul încheiat cu Abonatul precizează în mod expres aşa ceva,
- se supune auditurilor interne şi externe planificate, în special celor desfăşurate de personalul certSIGN sau celor aprobate de aceasta.

Pe lângă cele de mai sus, Autoritatea de Înregistrare se angajează:

- să se supună recomandărilor certSIGN, în special celor rezultate în urma auditurilor,
- să asigure protecţia datelor cu caracter personal, în concordanţă cu Legea nr. 677/2001 privind protecţia datelor cu caracter personal si cu Legea nr. 506/2004 privind prelucrarea

datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice ,

- să protejeze cheile private ale operatorilor în concordanţă cu cerinţele de securitate specificate în Codul de Practici şi Proceduri,
- să nu folosească cheile private ale operatorilor pentru alte scopuri decât cele prezentate în Codul de Practici şi Proceduri, cu excepţia cazului în care acest lucru este aprobat de certSIGN,
- să obţină din surse de încredere şi să verifice atent cheile publice active, certificatele şi CRL-urile Autorităţilor de Certificare aparţinând certSIGN.

2.1.3 Obligaţiile Abonaţilor

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

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

Prin contract, Abonatul final se angajează:

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

- să declare date corecte în aplicațiile trimise Autorității de Înregistrare sau unei Autorități de Certificare, care apoi sunt stocate în baza de date a certSIGN şi în certificate de chei publice emise; un Abonat trebuie să fie conştient de responsabilitățile ce îi revin pentru daunele directe şi indirecte provocate ca urmare a falsificării datelor;
- să accepte faptul că fiecare semnatura electronica creată prin intermediul unei chei private, aparținând Abonatului şi asociată unui certificat aprobat care conține cheie publică corespunzătoare, reprezintă semnatura Abonatului şi să recunoască faptul că certificatul nu a fost invalid (în afara datei de valabilitate) şi nici revocat sau suspendat atunci când a fost creată semnatura;
- să cunoască în general noțiunile referitoare la certificate, semnaturi electronice şi PKI.

De asemenea, Abonatul final se angajează:

- să se supună regulilor din prezentul Cod de Practici şi Proceduri şi Politica de certificare,
- să genereze cheile criptografice, să gestioneze parolele, cheile publice şi private, să schimbe informații cu Autoritatea de Înregistrare şi Autoritățile Certificare numai prin intermediul aplicațiilor software recomandate de către certSIGN; accesul la acest software, mediile şi dispozitivele pe care sunt stocate cheile şi parolele trebuie să fie controlat în mod adecvat,
- să considere pierderea sau dezvăluirea parolei (dezvăluirea parolei către o persoană neautorizată) ca o pierdere sau dezvăluire a cheii private (dezvăluirea acesteia către o persoană neautorizată),
- să nu permită accesul la cheile sale private persoanelor neautorizate,
- să nu folosească ca Abonat final o cheie privată asociată unui certificat emis de certSIGN, pentru semnarea de CRL-uri sau certificate,
- să facă dovada posesiei cheii private la Autoritatea de Înregistrare sau Certificare sau să demonstreze posesia acesteia în alt mod,
- să nu dezvăluie parolele persoanelor neautorizate,

- să transmită Autorității de Înregistrare documentele cerute care să confirme informațiile incluse în aplicația trimisă şi identitatea celui ce a transmis cererea sau a entității ce acționează în numele Abonatului,
- în cazul în care se constată încălcarea securității (sau există suspiciunea de încălcare a securității) cheilor private, să anunțe emitentul certificatului ,
- să folosească certificatele de chei publice şi cheile private corespunzătoare numai în scopurile declarate în certificat şi în concordanță cu ariile de aplicabilitate şi restricțiile stabilite prin Codul de Practici şi Proceduri
- să obțină certificate de chei publice ale Autorităților de Certificare şi Autorității de Înregistrare precum şi cele corespunzătoare altor servicii oferite de certSIGN.

2.1.4 Obligațiile Entităților Partenere

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

- furnizarea de servicii tip depozit, servicii de marcă temporala şi servicii de verificare a stării certificatelor (OCSP) – în cazul încheierii de contracte cu certSIGN;
- specificarea condițiilor pe care trebuie să le îndeplinească o semnatura electronica pentru a fi considerată validă de către o entitate parteneră – în cazul încheierii de contracte cu un Abonat;

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

Prin contract, Entitatea Parteneră se angajează:

- să fie de acord şi să respecte termenii şi condițiile din contract. Drepturile şi obligațiile părților încep să îşi producă efectele începând cu data încheierii contractului.
- să verifice cu atenție fiecare semnatura electronica de pe un certificat sau document recepționat. Pentru a verifica semnatura, entitatea parteneră trebuie:

- să specifice calea de certificare ce conţine toate certificatele Autorităţilor de Certificare care fac posibilă verificarea semnaturii de pe certificatul semnatarului,
- să se asigure că, din perspectiva creării semnaturii calea de certificare aleasă este cea mai bună; în unele cazuri, este posibil să existe mai mult de o cale pornind de la un certificat dat (prin intermediul căruia a fost creată semnatura) şi până la o Autoritate de Certificare pe care se bazează verificarea semnaturii.
- să verifice că nici unul din certificatele din calea de certificare, aparţinând certSIGN, nu se află în listele de certificate revocate sau suspendate;
- să verifice că toate certificatele din calea de certificare aparţin unor Autorităţi de Certificare şi că acestea sunt autorizate să semneze alte certificate,
- (opţional) să specifice data şi ora la care a fost semnat un document sau mesaj. Acest lucru este posibil numai dacă documentul sau mesajul a fost marcat (înainte de semnare) cu o marcă temporala emisă de o Autoritate de Marcare Temporala, sau semnaturii electronice i s-a asociat o marcă temporala imediat după semnarea documentului; o astfel de verificare permite implementarea de servicii de ne-repudiere sau se poate folosi pentru rezolvarea disputelor,
- să verifice, folosind o cale de certificare definită, credibilitatea certificatului semnatarului documentului sau mesajului şi autenticitatea semnaturii,

- să efectueze corect operaţiile criptografice, folosind aplicaţii software şi dispozitive având un nivel de securitate corespunzător nivelului de sensibilitate al certificatului procesat şi nivelului de credibilitate al certificatelor folosite,
- să considere o semnatura electronica ca fiind invalidă dacă prin mijloacele software sau dispozitivele folosite nu este posibil să se determine dacă semnatura electronica este validă sau dacă rezultatul verificării este negativ,
- verificarea semnaturii electronice îşi propune să stabilească dacă: (1) semnatura electronica a fost creată prin intermediul unei chei private corespunzătoare unei chei publice dintr-un certificat emis de certSIGN pentru un Abonat şi (2) mesajul (documentul) semnat nu a fost modificat după semnare.
- să aibă încredere numai în acele certificate de chei publice care:

- sunt folosite în concordanţă cu scopul declarat şi corespund ariilor de aplicabilitate specificate de entitatea parteneră, de exemplu, printr-o politică de semnatura (vezi Capitolul 1.4),
- a căror stare a fost verificată pe baza Listelor de certificate Revocate corespunzătoare, sau prin intermediul serviciului OSCP al certSIGN

- să specifice condiţiile pe care un certificat de cheie publică şi o semnatura electronica trebuie să le îndeplinească pentru a fi considerate valide; aceste condiţii pot fi formulate, de exemplu, sub forma unor politici de certificare acceptate şi apoi publicate.

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

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

2.1.5 Obligaţiile Depozitului

Depozitul este gestionat şi controlat de certSIGN; prin urmare, certSIGN se obligă:

- să depună toate eforturile pentru a se asigura că toate certificatele publicate în depozit aparţin Abonaţilor înscrişi în certificate, iar Abonaţii şi-au dat acordul asupra acestor certificate, conform cu cerinţele specificate în Capitolele 2.1.3. şi 4.3,
- să se asigure că certificatele Autorităţilor de Certificare, Autorităţii de Înregistrare aparţinând domeniului certSIGN precum şi certificatele Abonaţilor (după aprobarea lor) sunt publicate şi arhivate la timp,
- să asigure publicarea şi arhivarea Politicii de certificare, a Codului de Practici şi Proceduri, a listei aplicaţiilor şi dispozitivelor recomandate,
- să permită accesul la informaţiile despre starea certificatelor prin publicarea de Liste de certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogări HTTP,
- să asigure accesul permanent la informaţiile din depozit pentru Autorităţile de Certificare, Autoritatea de Înregistrare, Abonaţi şi Entităţile Partenere,

- să publice CRL-urile sau alte informații în timp util şi în concordanță cu termenele limită specificate în Politica de certificare,
- să asigure accesul sigur şi controlat la informațiile din depozit.

2.2 Răspunderea

Răspunderea părților ce oferă, sau utilizează servicii în domeniul gestionat de certSIGN, este stabilită prin contractele încheiate între acestea. Răspunderea părților intervine în cazul încălcării termenilor şi condițiilor stipulate în contractele încheiate sau în alte documente ce au legătură cu aceste contracte. În situații excepționale, dacă şi contractul prevede acest lucru, o parte din răspunderea juridică a unei părți poate fi preluată sau delegată unei alte părți. O asemenea situație poate apare în cazul în care o Autoritate de Certificare deleagă responsabilitatea verificării identității Abonaților către Autoritatea de Înregistrare. Autoritatea de Înregistrare este responsabilă pentru obligațiile ce îi revin, obligații specificate în Capitolul 2.1.2.

certSIGN este responsabilă din punct de vedere juridic pentru consecințele acțiunilor întreprinse de Autoritățile de Certificare ***certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3***, ***certSIGN Enterprise CA Class 3*** *şi* ***certSIGN Non-Repudiation CA Class 4****, de Autoritatea de Înregistrare, de Depozit şi, în cazul în care contractele prevăd acest lucru, de alte Autorități de Certificare.*

Răspunderea juridică, nu elimină şi nici nu substituie răspunderea ce decurge din contractele încheiate între părți sau din acte normative.

2.2.1 Răspunderea Autorităților de Certificare

Autoritățile de Certificare aparținând certSIGN răspund din punct de vedere juridic în cazul în care prejudiciile directe sau indirecte provocate Abonaților sau Entităților Partenere:

- apar în ciuda faptului că acestea au respectat termenii şi condițiile stabilite în Politica de Certificare şi Codul de Practici şi Proceduri,
- apar datorită erorilor certSIGN, precum: discrepanțele dintre procesul efectiv de verificare a identității şi procedurile declarate, protecția neadecvată a cheilor private ale

Autorităților de Certificare, imposibilitatea de a accesa serviciile oferite (de exemplu, la CRL-uri), numai dacă se probează culpa certSIGN.

- apar ca urmare a încălcării obligațiilor certSIGN, specificate în Capitolele 2.1.1, numai în cazul în care culpa certSIGN este probată.

Abonatul declară şi este singurul responsabil asupra următoarelor:

- datele şi documentele prezentate Autorității de Înregistrare sunt autentice şi exacte,
- prin acceptarea unui certificat, acceptă faptul că certificatul nu conține greşeli datorate neglijenței sau încălcării procedurilor de către persoanele care prelucrează cererile de certificat, sau cele care eliberează certificatele.

certSIGN nu va încheia nici un contract cu Abonații care nu acceptă aceste declarații, în cazul în care are cunoştință de existența vreunuia dintre cazurile prezentate mai sus.

certSIGN nu îşi asumă nici o responsabilitate pentru acțiunile Entităților Partenere, Abonaților sau ale altor părți care nu sunt asociate cu certSIGN. certSIGN nu este responsabilă pentru:

- daunele cauzate de forța majoră şi / sau cazul fortuit. Se înțelege prin caz de forță majoră acel eveniment imprevizibil şi de neînlăturat produs ulterior perfectării contractului precum: incendiu, cutremur, orice altă calamitate naturală, precum şi războiul. Împrejurarea relativ imprevizibilă şi relativ invincibilă, neavând caracter extraordinar, precum: grevele, restricțiile legale, alte asemenea evenimente, definesc cazul fortuit;
- daunele cauzate de instalarea şi utilizarea aplicațiilor sau dispozitivelor folosite pentru generarea şi gestionarea cheilor criptografice, criptare, creare de semnaturi electronice, care nu îndeplinesc condițiile specificate la pct. 1.4.1,
- daunele cauzate de utilizarea necorespunzătoare a certificatelor emise („necorespunzător” reprezintă utilizarea unui certificat revocat sau suspendat sau în neconcordanță cu scopul declarat al certificatului, specificat în prezentul Cod de Practici şi Proceduri),
- situația în care un certificat nu a fost aprobat de Abonat, iar acest lucru a fost confirmat de către Abonatul respectiv, răspunderea revine Abonatului,

- stocarea de date eronate în bazele de date ale certSIGN şi includerea acestora în certificate digitale emise Abonatului în cazul în care Abonatul a declarat că aceste date sunt corecte.

2.2.2 Responsabilitățile Autorității de Înregistrare

Responsabilitățile Autorității de Înregistrare sunt preluate automat de către certSIGN ca urmare a obligațiilor stipulate în Capitolele 2.1.1, 2.1.2, 2.1.5. Condițiile în care sunt preluate aceste responsabilități sunt stabilite de contractele încheiate de certSIGN cu Abonații şi Entitățile Partenere (daca este cazul).

În cazul în care Autoritatea de Înregistrare nu face verificările necesare în cazul unui Abonat care a declarat cele specificate în Capitolul 2.2.1, întreaga răspundere juridică ce rezultă din încălcarea obligațiilor descrise în Capitolul 2.1.2 aparține Autorității de Înregistrare.

2.2.3 Răspunderea Abonaților

Răspunderea juridică a Abonaților rezultă din obligațiile şi garanțiile specificate în Capitolul 2.1.3. Condițiile în care intervine această răspundere sunt stipulate în contractul încheiat de abonat cu certSIGN.

2.2.4 Răspunderea Entităților Partenere

Răspunderea juridică a Entităților Partenere rezultă din drepturile şi obligațiile stipulate în Capitolul 2.1.4. Condițiile în care intervine răspunderea sunt stipulate în contractul încheiat de Entitățile Partenere cu certSIGN, sau cu un Abonat.

Conform prevederilor contractelor încheiate de Entitățile Partenere cu Abonații şi certSIGN este necesar ca Entitățile Partenere să confirme că dețin suficiente informații pentru a putea lua o decizie cu privire la acceptarea sau respingerea unei semnaturi electronice, în momentul verificării acesteia.

În contractele încheiate, părțile trebuie să specifice valoarea tranzacțiilor financiare acceptate de acestea numai pe baza informațiilor cuprinse într-un certificat digital şi să dea o declarație prin

care să afirme că sunt conştienţi de consecinţele legale ce decurg din nerespectarea obligaţiilor descrise în prezentul Cod de Practici şi Proceduri.

2.2.5 Răspunderea Depozitului

Răspunderea pentru modul de funcţionare al Depozitului şi consecinţele funcţionării acestuia, aparţine certSIGN (vezi Capitolul 2.2.1).

2.3 Responsabilităţi de natură financiară

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

2.4 Legea aplicabilă. Durata. Aplicabilitate. Alte rezoluţii

2.4.1 Legea aplicabilă

Legea aplicabilă prezentului Cod de Practici şi Proceduri este legea română. Toate activităţile desfăşurate în baza prezentului document vor respecta dispoziţiile prevăzute de actele normative în vigoare din România, în domeniul serviciilor de certificare.

Obligaţiile certSIGN rezultă din obligaţiile asumate în baza prezentului Cod de Practici şi Proceduri.

2.4.2 Intrarea în vigoare. Durata

2.4.2.1 Intrarea în vigoare. Durata. Modificarea clauzelor

Prevederile prezentului Cod de Practici şi Proceduri intră în vigoare la data notificarii către Autoritatea de Reglementare şi Supraveghere şi sunt valabile până la data unei noi versiuni.

Modificările prevederilor prezentului CPP, sau introducerea de noi prevederi se desfăşoară în concordanţă cu procedurile prezentate în Capitolul 8.

2.4.2.2 Excepţii de la durata de valabilitate

Dacă înţelegerile încheiate pe baza prezentului Cod de Practici şi Proceduri conţin clauze de confidenţialitate asupra conţinutului, clauze privind confidenţialitatea informaţiilor deţinute de părţi, clauze referitoare la respectarea drepturilor de copyright, sau drepturilor de autor, aceste clauze sunt considerate în vigoare şi după expirarea perioadei de valabilitate a înţelegerii dintre părţi, pentru o perioadă care se va defini la momentul realizarii intelegerii respective si cu respectarea normelor legale in vigoare.

2.4.3 Aplicabilitate

Prevederile prezentului Cod de Practici şi Proceduri sunt aplicabile părţilor, aşa cum sunt acestea menţionate la capitolul 2.1 şi Abonaţilor care încheie contracte în conformitate cu prevederile prezentului CPP.

2.4.4 Independenţa clauzelor

În cazul în care una dintre prevederile prezentului Cod de Practici şi Proceduri sau ale contractelor ce au fost încheiate în baza lui, este considerată de către o instanţă sau de către orice altă autoritate competentă ca fiind nulă sau neaplicabilă, prevederea respectivă se va considera a fi eliminată din prezentul Cod de Practici şi Proceduri sau contractele ce au fost încheiate în baza lui, iar celelalte prevederi ale Codului de Practici şi Proceduri sau ale contractelor încheiate vor rămâne valabile şi aplicabile şi vor continua să se aplice ca atare.

2.4.5 Trimiteri

Prezentul Cod de Practici şi Proceduri şi contractele ce au fost încheiate în baza acestuia pot conține referințe la alte dispoziții, cu condiția ca:

- acest lucru să fie stipulat ca o clauză în Cod sau în contract
- respectivele prevederi la care se face referire în Cod sau în contract să fie dispoziții scrise.

2.4.6 Notificări

Părțile menționate în prezentul Cod de Practici şi Proceduri pot defini, pe baza înțelegerilor, metodele de notificare reciprocă. Dacă aceste metode nu sunt definite, prezentul Cod permite schimbul de informații utilizându-se poşta electronica, faxul, telefonul, protocoalele de rețea (TCP/IP, HTTP) etc.

Alegerea mijloacelor de comunicare poate fi condiționată de tipul de informații vehiculate. De exemplu, majoritatea serviciilor furnizate de certSIGN necesită utilizarea unuia sau mai multor protocoale de rețea permise. Anumite informații şi notificări trebuie furnizate în concordanță cu un orar definit. Acest lucru se aplică în special publicării CRL-urilor, noilor certificate ce aparțin Autorității de Înregistrare şi Autorităților de Certificare şi informării Abonaților sau Entităților Partenere (dacă aşa este stipulat în contracte) despre aceasta, precum şi informarea legată de periclitarea cheii private a oricărei Autorități de Certificare operată de certSIGN.

Orice comunicare între părți, referitoare la îndeplinirea prezentului contract, trebuie să fie transmisă în scris. Orice document scris trebuie înregistrat atât în momentul transmiterii, cât şi în momentul primirii. Comunicările dintre părți se pot face şi prin telefon, telegrama, telex, fax, sau email, cu condiția confirmării în scris a primirii comunicării.

2.4.7 Soluționarea litigiilor

Părțile implicate în contract vor încerca soluționarea pe cale amiabilă a eventualelor litigii apărute.

În cazul în care între părți se naşte un diferend cu privire la neîndeplinirea obligațiilor asumate, părțile vor încerca soluționarea prin conciliere directă a respectivului diferend. În cadrul

concilierii directe, fiecare parte se va folosi de orice mijloc de apărare admis de legislația în vigoare pentru susținerea punctelor de vedere.

Orice diferend cu privire la intrarea în vigoare, interpretarea, executarea şi încetarea prezentului Cod de Practici şi Proceduri şi nesoluționat pe cale amiabilă va fi deferit instanțelor judecătoreşti de drept comun, spre competentă soluționare, conform normelor legislative româneşti în vigoare.

Limba care guvernează prezentul Cod de Practici şi Proceduri este limba română, iar documentul va fi interpretat conform legilor din România.

2.5 Prețul serviciilor. Modalitatea de plată

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

Serviciile oferite de certSIGN sunt stabilite după cum urmează:

- **servicii de certificare individuale** – prețul este stabilit pentru fiecare serviciu în parte, de exemplu, pentru fiecare certificat vândut sau un număr mic de certificate,
- **pachete de servicii de certificare** – prețul este stabilit pentru pachete de servicii prestate unei singure entități,
- **servicii prestate pe baza de abonament** – prețul este stabilit pentru servicii prestate lunar; valoarea sumelor plătite depinde de tipul şi numărul serviciilor accesate şi este utilizat în special pentru serviciile de marcare temporala şi de verificare a stării certificatelor prin intermediul protocolului OCSP,
- **servicii indirecte –** prețul este stabilit pentru fiecare serviciu oferit clienților săi de un partener certSIGN, care îşi bazează activitatea pe infrastructura certSIGN; de exemplu, dacă o Autoritate de Certificare comercială este certificată de certSIGN, atunci certSIGN va percepe un preț pentru fiecare certificat emis de Autoritatea de Certificare respectivă.

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

2.5.1 Valoarea serviciilor de eliberare şi reînnoire a certificatelor digitale

Având în vedere diferența dintre procedurile de eliberare şi reînnoire a unui certificat, valoarea serviciilor de eliberare sau reînnoire a unui certificat digital (vezi 2.5), corespunzătoare modelelor prezentate anterior pot fi împărțite în trei componente: (1) valoarea serviciilor de identificare şi autentificare sau valoarea serviciilor desfăşurate de Autoritatea de Înregistrare (2) valoarea serviciilor de eliberare a certificatelor digitale şi (3) valoarea serviciilor de personalizare şi eliberare a dispozitivelor criptografice (token). Aceste componente pot fi cotate separat într-o listă de prețuri şi utilizate în cazul reînnoirii certificatelor (costurile de identificare, autentificare a Abonatului şi cele de personalizare si eliberare de token-uri pot fi omise în cazul reînnoirii).

2.5.2 Valoarea serviciilor de acces la certificate

Valoarea serviciilor de acces la certificate în anumite condiții speciale cerute de Entitățile Partenere se stabileşte conform modalităților aplicate serviciilor prestate pe baza de abonament şi serviciilor indirecte.

Valoarea acestor servicii se stabileşte în contractele încheiate cu entitățile partenere şi depinde de tipul de certificat emis.

2.5.3 Valoare serviciilor de revocare sau acces la informațiile despre starea certificatelor

Serviciile de revocare a unui certificat, de publicare a certificatelor în CRL, sau accesul la CRL-urile publicate în depozit (sau în alte locații) sunt gratuite.

certSIGN poate stabili prețuri pentru serviciile de verificare a stării certificatelor, prin intermediul protocolului OCSP sau a altor sisteme. În acest caz, prețurile se vor calcula conform prețurilor stabilite pentru serviciile de certificare individuale sau serviciilor prestate pe bază de abonament.

Fără aprobarea scrisă a certSIGN, este interzisa pentru terţele părţi care oferă servicii de verificare a stării certificatelor utilizarea informatiilor din CRL sau a informaţiilor despre starea certificatelor. Utilizarea acestor informatii este permisa numai după semnarea unui contract cu certSIGN. În acest caz, valoarea serviciului va fi calculata după modelul serviciului indirect de vânzare (de exemplu, este stabilită o sumă pentru fiecare confirmare referitoare la starea unui certificat, emisă de terţa parte).

2.5.4 Alte preţuri

certSIGN poate presta şi alte servicii contra cost (vezi 2.5) cum ar fi:

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

2.5.5 Rambursarea plăţilor

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

Cererile de rambursare trebuie trimise la adresa specificată în Capitolul 1.5.

2.6 Depozitul şi publicarea informațiilor

2.6.1 Informațiile publicate de către certSIGN

Depozitul (repository) este o interfață publică către următoarele informații:

- versiunea curentă şi cea anterioară a Politicii de certificare şi a Codului de Practici şi Proceduri
- Modelele de contract cu Abonații şi Entitățile Partenere,
- Declarația certSIGN cu privire la asigurarea confidențialității informațiilor recepționate şi procesate
- Registrul (în accepțiunea legii semnaturii electronice)
- certificatele certSIGN ROOT CA, certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class3, certSIGN Enterprise CA Class 3 şi certSIGN Non-Repudiation Class 4 precum şi certificatele tuturor Autorităților de Certificare care aparțin sau sunt legate la domeniul certSIGN (de exemplu, certificatele Autorităților de Certificare noi înregistrate de RA),
- certificatele abonaților finali (entități fizice şi juridice, inclusiv angajații certSIGN şi maşinile / aplicațiile software deținute de aceştia şi care sunt indispensabile pentru serviciile PKI) conform Legii semnaturi electronice.

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

- Listele de certificate Revocate (CRL); CRL-urile sunt disponibile în aşa numitele puncte de distribuție a CRL-urilor, a căror adresă este specificată în fiecare certificat emis de certSIGN; locația principala de distribuție a CRL-urilor este în depozit la adresa: http://crl.certsign.ro,
- Alte informații ce se modifică în timp real,

Conținutul depozitului este disponibil prin Internet la adresa: http://www.certsign.ro/repository sau prin intermediul protocolului LDAP v3, la adresa ldap.certsign.ro, port 389

2.6.2 Frecvența publicării

Informațiile publicate de certSIGN sunt actualizate cu următoarea frecvență:

- Politica de Certificare şi Codul de Practici şi Proceduri – vezi Capitolul 8,
- certificatele Autorităților de Certificare din cadrul certSIGN – după emiterea unui nou certificat;
- certificatul Autorității de Înregistrare – după emiterea unui nou certificat;
- certificatele Abonaților – după fiecare emitere a unui nou certificat,;
- Lista certificatelor Revocate – vezi Capitolul 4.9.4;
- Rapoartele de audit efectuate de instituțiile autorizate – în momentul în care certSIGN intră în posesia lor;
- Informațiile suplimentare – după fiecare actualizare.

2.6.3 Accesul la informațiile publicate de certSIGN

Toate informațiile publicate de certSIGN în depozit la adresa http://www.certsign.ro/repository sunt accesibile public.

certSIGN a implementat mecanisme logice şi fizice de protecție împotriva adăugării, ştergerii şi modificării informațiilor publicate în depozit.

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

2.7 Auditul

Auditurile au ca obiectiv verificarea consistenței acțiunilor certSIGN sau a entităților delegate de aceasta cu declarațiile şi procedurile acestora (inclusiv Politica de certificare şi Codul de Practici şi Proceduri).

Auditurile desfăşurate de certSIGN urmăresc în principal centrele de procesare a datelor şi procedurile de gestiune a cheilor. De asemenea, aceste audituri au în vedere şi Autoritățile de

Certificare de pe calea de certificare a **certSIGN ROOT CA**, Autoritatea de Înregistrare sau alte elemente ale infrastructurii de chei publice, cum ar fi de exemplu serverele OCSP.

Auditurile desfăşurate de certSIGN pot fi efectuate de echipe interne (audit intern) sau de organizații independente (audit extern). În ambele cazuri, auditul se desfăşoară la cererea şi sub supravegherea administratorului de securitate (vezi Capitolul 5.2.1).

2.7.1 Frecvența auditării

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

2.7.2 Identitatea / calificările auditorului

Auditul extern este realizat de către o instituție românească autorizată şi independentă față de certSIGN sau de către o instituție internaționala având reprezentanță sau orice sediu secundar în România. O asemenea instituție trebuie să:

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

Auditul intern este realizat de către departamentul de calitate şi audit al certSIGN.

2.7.3 Relația auditorilor cu entitatea auditată

Vezi 2.7.2.

2.7.4 Domeniile supuse auditării

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

- securitatea fizică a certSIGN,
- procedurile de verificare a identității Abonaților,

- serviciile de certificare şi procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software şi a accesului la rețea,
- securitatea personalului certSIGN,
- jurnalele de evenimente şi procedurile de monitorizare a sistemului,
- arhivarea şi restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru certSIGN,
- înregistrările referitoare la analizele şi verificările efectuate pentru aplicațiile software şi dispozitivele hardware.

2.7.5 Măsurile întreprinse ca urmare a descoperirii unei deficiențe

Rezultatele auditurilor interne şi externe sunt transmise managementului certSIGN. În termen de 14 zile de la transmiterea rezultatelor, acesta trebuie să pregătească o opinie scrisă cu privire la deficiențele sesizate şi să propună un plan de acțiune şi termene de rezolvare, pentru eliminarea deficiențelor. Informațiile referitoare la modul de rezolvare a deficientelor vor fi trimise auditorului.

În cazul deficiențelor ce reprezintă o amenințare directă asupra procesului de certificare al ***certSIGN Qualified CA Class 3, certSIGN Enterprise CA Class 3*** *şi* ***certSIGN Non-Repudiation CA Class 4****, administratorul de securitate poate lua decizia suspendării temporare a activității acestora. Toți clienții certSIGN vor fi anunțați de măsura luată şi timpul estimativ în care autoritatea respectivă îşi va relua activitatea. Notificarea se poate face prin intermediul depozitului, prin e-mail şi – în cazuri absolut necesare – prin publicarea în presă.*

2.8 Confidențialitatea şi caracterul privat al informațiilor

Toate informațiile pe care le deține certSIGN au fost obținute, păstrate şi procesate în concordanță cu legile în vigoare, în mod special cu Legea românească privind protecția datelor

cu caracter personal (Legea 677/2001) şi cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice. Relaţiile dintre un Abonat, o entitate parteneră şi certSIGN se bazează pe încredere.

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

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

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

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

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

sau

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

sau

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

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

2.8.1 Tipuri de informaţii considerate ca fiind private sau confidenţiale

certSIGN, angajaţii acesteia precum şi entităţile care desfăşoară activităţi de certificare sunt obligate să păstreze secretul informaţiilor, atât pe durata, cât şi după încetarea contractului de muncă, în cazul angajaţilor. Sunt catalogate drept informaţii private sau confidenţiale:

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

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

2.8.2 Tipuri de informaţii care nu sunt considerate ca fiind private sau confidenţiale

Toate informaţiile necesare bunei funcţionări a serviciilor de certificare nu sunt considerate ca fiind confidenţiale sau private. În particular, acest lucru se referă la informaţiile incluse într-un

certificat de către Autoritățile de Certificare emitente, în concordanță cu specificațiile din Capitolul 7. Un Abonat care aplică pentru obținerea unui certificat cunoaşte ce fel de informații vor fi incluse în certificat şi este de acord cu publicarea acestora.

O parte din informațiile furnizate de, sau către Abonați poate fi pusă la dispoziția altor entități, doar cu acordul scris al Abonatului şi în scopul menționat în contractul încheiat cu Abonatul.

Următoarele categorii de informații, trimise către Autoritățile de Certificare şi Autoritatea de Înregistrare, sunt accesibile public în depozit:

- Politica de certificare şi Codul de Practici şi Proceduri,
- lista de prețuri pentru serviciile oferite,
- ghiduri pentru utilizatori,
- certificatele Autorității de Înregistrare şi Autorităților de Certificare,
- certificatele Abonaților (după obținerea aprobării acestora),
- lista certificatelor revocate (CRL),
- informații referitoare la cursurile de instruire ținute de certSIGN.

2.8.3 Dezvăluirea motivului pentru care un certificat a fost revocat

Dacă un certificat a fost revocat la cererea unei părți autorizate (nu de către partea căreia i se revocă certificatul), informațiile cu privire la revocare şi motivele acestei revocări sunt comunicate ambelor părți.

2.8.4 Dezvăluirea informațiilor confidențiale către autoritățile legale

Informațiile confidențiale pot fi dezvăluite reprezentanților autorităților legale numai după îndeplinirea tuturor formalităților cerute de legislația în vigoare în România.

2.8.5 Dezvăluirea informațiilor confidențiale la cererea proprietarului

Prezentul Cod de Practici şi Proceduri nu precizează nici o condiție în acest sens.

2.8.6 Alte circumstanțe cu privire la dezvăluirea informațiilor

Prezentul Cod de Practici şi Proceduri nu precizează nici o condiție în acest sens.

2.9 Drepturile de proprietate intelectuală

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

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

Fiecare pereche de chei asociata unui certificat emis de certSIGN este proprietatea subiectului acelui certificat, specificat în câmpul *Subject* al certificatului (vezi Capitolul 7.1), cu excepţia certificatelor profesionale, caz în care proprietarul este persoană juridică.

3 Identificarea şi autentificarea

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

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

3.1 Înregistrarea inițială

Înregistrarea Abonatului are loc atunci când un Abonat care cere înregistrarea nu deține un certificat valid emis de nici o Autoritate de Certificare afiliată la certSIGN.

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

Fiecare Abonat este supus unui proces de înregistrare o singură dată. După verificarea datelor puse la dispoziție de un Abonat, acesta este inclus pe lista utilizatorilor autorizați ai serviciilor certSIGN şi i se acordă un certificat de cheie publică.

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

- completeze un formular de înregistrare disponibil on-line, sau ca document ce poate fi downloadat de pe site-ul Web al certSIGN,
- genereze o pereche de chei asimetrice RSA şi să furnizeze Autorității de Înregistrare, dovada deținerii unei chei private; opțional, Abonatul poate să însărcineze o Autoritate de Certificare sau Autoritatea de Înregistrare cu generarea acestei perechi de chei,
- sugereze un nume distinctiv (ND, vezi Capitolul 3.1.1),
- completeze şi să trimită un formular de înregistrare care conține o cheie publică şi dovada posesiei cheii private corespunzătoare acesteia,

- să se prezinte, opțional, la Autoritatea de Înregistrare şi să furnizeze documentele necesare (dacă se cere acest lucru de politica de certificare pe baza căreia se emite certificatul),
- încheie un contract cu un agent al Autorității de Înregistrare în legătură cu furnizarea serviciilor de către certSIGN; prezentul Cod de Practici şi Proceduri este parte integrantă a acestui contract.

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

3.1.1 Tipuri de nume

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

Pentru a asigura o comunicare electronica facilă cu Abonatul, în certificatele certSIGN este folosit un nume suplimentar pentru Abonat. Acest nume poate de asemenea să conțină adresa de e-mail a Abonatului, în concordanță cu recomandările RFC 822.

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

3.1.2 Necesitatea ca numele să aibă un înțeles

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

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

- câmpul C – abrevierea internațională pentru numele țării (RO pentru România),
- câmpul S – județul / sectorul în care locuieşte Abonatul,
- câmpul L – oraşul în care Abonatul are domiciliul,
- Street – adresa,
- câmpul CN – numele Abonatului; numele unui produs sau echipament poate de asemenea să fie specificat aici,
- câmpul O – numele instituției în cadrul căreia lucrează Abonatul, în cazul în care certificatul este profesional
- câmpul OU – numele departamentului în care este angajat Abonatul, în cazul în care certificatul este profesional
- câmpul T – funcția
- câmpul SN – numele de familie al Abonatului,
- câmpul G – prenumele Abonatului,
- câmpul P – pseudonimul Abonatului pe care acesta îl foloseşte în mediul său, sau pe care doreşte să îl folosească pentru a nu-şi descoperi numele sau prenumele real,
- câmpul Phone – numărul de telefon,
- câmpul Serial Number – codul personal de identificare al Abonatului în sensul Legii semnaturii digitale.

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

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

Numele Abonatului trebuie confirmat de un operator al Autorității de Înregistrare şi aprobat de o Autoritate de Certificare. certSIGN asigură (în cadrul domeniului său) unicitatea ND-urilor.

3.1.3 Reguli de interpretare a diferitelor formate de nume

Interpretarea câmpurilor din certificatele emise de certSIGN se face în concordanță cu profilele de certificate descrise în Profilul certificatelor şi al CRL-urilor (Capitolul 7). În crearea şi interpretarea ND-ului se face apel la recomandările specificate în Capitolul 3.1.2.

3.1.4 Unicitatea numelor

Identificarea fiecărui deținător de certificate emise de certSIGN se realizează pe baza ND-ului. *certSIGN asigură unicitatea ND-ului asignat fiecărui Abonat.*

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

Dacă un ND sugerat de Abonat încalcă drepturile altor entități la acest nume (vezi Capitolul 3.1.5), certSIGN poate adăuga alte atribute ND-ului (ex. numărul serial), care asigură unicitatea acestui nume în cadrul domeniului certSIGN. Un Abonat este îndreptățit să refuze un ND sugerat în procedura specificată în Capitolul 4.4.

Formatul numelui unic global pentru un Abonat are următoarea formă:

certSIGN.ro / numele emitentului / numele Abonatului

în care **certSIGN.ro** este numele domeniului certSIGN, numele emitentului este ND-ul uneia din Autoritățile de Certificare şi numele Abonatului este ND-ul câmpului *subject* din certificat. Valorile ultimelor două câmpuri sunt extrase din certificat.

Dacă un Abonat renunță la serviciile certSIGN, eventuala cererea de atribuire a ND-ului său altui Abonat trebuie respinsă.

certSIGN poate înregistra un Abonat cu un Nume Distinctiv folosit în trecut de alt Abonat numai cu acordul scris al acestuia din urmă.

3.1.5 Procedura de rezolvare a conflictelor privind revendicarea numelui

Numele care nu aparțin unui Abonat nu pot fi folosite în cererile sale de certificat. certSIGN nu verifică dacă un Abonat este îndreptățit să folosească numele menționat în cererea de înregistrare şi nici nu intenționează să-şi asume rolul de arbitru în rezolvarea disputelor privind drepturile de proprietate asupra oricărui Nume Distinctiv, marcă comercială sau nume comercial.

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

3.1.6 Dovada posesiei cheii private

Dacă o entitate deține o cheie privată când cere emiterea unui certificat, Autoritățile de Certificare şi Autoritatea de Înregistrare care funcționează în cadrul certSIGN trebuie să se asigure că entitatea deține o cheie privată corespunzătoare cheii publice furnizate.

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

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

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

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

Cheile private se recomandă a fi generate în interiorul unui dispozitiv criptografic (token) sau, în cazul generării lor în afara token-ului, prin intermediul unui generator software sau hardware urmând ca apoi să fie importate pe token. Orice entitate poate deține un token la momentul generării şi importului cheii, sau token-ul poate fi furnizat entității după procesul de generare de cheie. În ultimul caz, certSIGN garantează că token-ul şi cheia vor ajunge în mod sigur, direct la entitatea respectivă (vezi Capitolul 6.1.2).

3.1.7 Autentificarea identității persoanelor juridice

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

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

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

Autentificarea identității unei persoane juridice se poate face fie prin prezența personală a reprezentantului autorizat al persoanei juridice la Autoritatea de Înregistrare, fie prin prezența în

persoană a reprezentantului autorizat al Autorității de Înregistrare la sediul persoanei juridice (specificat în cerere).

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

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

Procedura de verificare la RA a identității persoanei juridice şi a identității reprezentantului său autorizat constă în (vezi de asemenea şi Tabelul 3.1.8):

- verificarea documentelor furnizate de Abonat,
- verificarea cererii, care constă în:
  - verificarea conformității datelor menționate în cerere cu cele din documentele furnizate,
  - (opțional) verificarea dovezii posesiei cheii private (dacă cererea implică o pereche de chei pentru crearea unei semnaturi electronice) şi măsura în care Numele Distinctiv este cel potrivit,
- verificarea autorizației şi identității reprezentantului persoanei juridice care trimite cererea (inclusiv cereri de acreditare ca Autoritate de Certificare) în numele acestei entități.
- 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 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 RA daca abonatul nu isi valideaza contul de email.

Autoritatea de Înregistrare se angajează să verifice corectitudinea şi autenticitatea tuturor datelor furnizate într-o cerere (vezi Tabelul 3.1.8, Capitolul 3.1.9).

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

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

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

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

- identitatea operatorului Autorității de Înregistrare care verifică identitatea solicitantului,
- trimiterea declarației operatorului (semnată de mână) prin care se atestă faptul că acesta a verificat identitatea solicitantului în concordanță cu cerințele prezentului Cod de Practici şi Proceduri,
- data verificării,

- identificatorul operatorului şi al solicitantului în cazul în care acesta din urmă este prezent în persoană la Autoritatea de Înregistrare (presupunând că solicitantului i s-a atribuit un astfel de identificator),
- declarația solicitantului (semnată de mână) cu privire la corectitudinea datelor incluse în cerere, în concordanță cu cerințele prezentului Cod de Practici şi Proceduri,

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

3.1.8 Autentificarea identității persoanelor fizice

Autentificarea identității persoanelor fizice (entități private) are două scopuri. Autentificarea trebuie să dovedească (1) că datele dintr-o cerere se referă la o entitate privată existentă şi (2) că solicitantul este într-adevăr entitatea privată menționată în cerere.

Autentificarea persoanelor fizice se realizează pe baza:

- documentelor (carte de identitate sau paşaport) care confirmă identitatea solicitantului,

şi dacă Abonatul doreşte să includă datele unei instituții (persoană juridică) pentru care lucrează:

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

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

- verificarea documentelor furnizate de Abonat (carte de identitate sau paşaport in original sau copie legalizata), inclusiv bazele de date ale CA sau ale altor instituții,
- verificare cererii înaintate:
  - verificarea consecvenței datelor din cerere cu cele din documente,
  - (opțional) verificarea dovezii posesiei unei chei private şi a gradului de potrivire a ND-ului.
- verificarea setului de informații din cerere folosind alte surse (Registrul Comerțului din România, Registrul de Evidență a Populației etc.).

- verificarea faptului ca contul de mail care apare in cererea de certificat este controlat de catre abonat. Cererea de certificat nu poate fi facuta/validata in aplicatia software RA daca abonatul nu isi valideaza contul de email.

Cerințele verificării identității unei entități private depind de nivelul certificatului (Tabelul 3.1.8)

Politica de certificare	Cerințe Operatorii Autorității de Înregistrare compară datele Abonatului primite prin una din variantele:
certSIGN Clasa 1	**A. În cazul certificatelor personale demonstrative:**
	• se verifică adresa de e-mail prin trimiterea instrucțiunilor de instalare a certificatelor la această adresă menționată în cerere.
	B. În cazul certificatelor Entreprise demo sau Non-repudiation demo operatorii Autorității de Înregistrare compară datele primite de la Abonat prin una din următoarele variante:
	• prin fax (varianta recomandată),
	• prin poşta electronica cu fişier ataşat: gif, tif, jpg, bmp (opțional), cu datele trimise la Autoritatea de Înregistrare / Certificare de către Abonat
certSIGN Clasa 2	• prin fax (varianta recomandată)
	• printr-o scrisoare (opțional)
	• prin prezență în persoană (opțional),
	• prin poşta electronica cu fişier ataşat: gif, tif, jpg, bmp (opțional)
certSIGN Clasa 3	• prin prezența personală la Autoritatea de Înregistrare (varianta recomandata)
	• printr-o scrisoare care trebuie să conțină copii ale documentelor originale confirmate de un notar (opțional)
	• în format electronic, care trebuie să conțină copii ale documentelor originale autentificate de un notar în condițiile legii notarului electronic nr 589/15.12.2004 (opțional)
certSIGN Clasa 4	• prin prezența personală la Autoritatea de Înregistrare (varianta recomandată)
	• printr-o scrisoare care conține copii ale documentelor originale confirmate de un notar (opțional),
	• în format electronic, care trebuie să conțină copii ale documentelor originale autentificate de un notar în condițiile legii notarului electronic nr 589/15.12.2004 (opțional)

Tabel 3.1.8. Cerințele impuse în procesul de verificare a identității unei persoane fizice/juridice

3.1.9 Autentificare originii dispozitivelor

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

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

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

Verificarea informațiilor care se înregistrează depinde de nivelul de credibilitate al certificatului. Sunt două metode de autentificare a originii unui dispozitiv şi a integrității datelor furnizate:

- verificarea cererii semnate electronic trimise de un sponsor (cererea trebuie semnată cu o cheie privată asociată cu un certificat cu un nivel de credibilitate egal sau mai mare decât al certificatului solicitat),
- în timpul înregistrării personale de către sponsor a unui dispozitiv; identitatea sponsorului este confirmată în concordanță cu cerințele stipulate în Capitolul 3.1.8.

3.1.10 Autentificarea autorizațiilor

Autoritatea de Înregistrare şi Autoritățile de Certificare certSIGN pot confirma autorizarea unei persoane fizice de a acționa în numele altor entități, de obicei persoane juridice. Asemenea autorizații sunt, de obicei, asociate cu un anumit rol în instituție,

Autentificarea autorizațiilor este parte a procedurii întreprinse de Autoritatea de Înregistrare sau de Autoritatile de Certificare pentru procesarea cererii de certificat pentru o persoană juridică, sau pentru un dispozitiv aparținând unei persoane juridice sau fizice. În ambele cazuri, emiterea certificatului este o confirmare a faptului că o persoană juridică sau un dispozitiv au dreptul să folosească cheia privată în numele persoanei juridice.

Autorizarea este delegată de către o persoană juridică, fie către angajații săi, fie către o terță parte împuternicită de aceasta. Procedura de autentificare a autorizațiilor adoptată de certSIGN conține, în afară de autentificarea autorizației şi autentificarea persoanei fizice către care aceste autorizații sunt delegate. Această cerință poate fi omisă numai dacă entitatea este deja Abonat certSIGN. Autentificarea identității persoanei fizice este realizată în modul descris în Capitolul 3.1.8.

Procedura de autentificare a autorizației cuprinde:

- verificarea autenticității cererii înaintate,
- verificarea conformității datelor persoanei juridice prezente în cerere cu cele din documentele înaintate,

- (opţional) verificarea dovezii posesiei cheii private (dacă cererea se referă la o pereche de chei pentru crearea de semnaturi) şi gradul de potrivire a ND-ului persoanei juridice şi a persoanei fizice care poate acţiona în numele acestei persoane juridice,
- existenţa unui document emis de cel puţin un membru al consiliului de administraţie şi care confirmă autorizarea persoanei fizice; documentul trebuie certificat de un notar,
- contactarea superiorului direct al persoanei fizice care să confirme autorizaţia.

3.1.11 Marci Inregistrate

"Certsign nu verifica daca Abonatul (utilizatorul/titularul unui certificat) este persoana în numele căreia marca este înregistrată în Registrul Naţional al Mărcilor sau daca beneficiaza de dreptul, acordat de titularul marcii, de utilizare a acesteia, Abonatul fiind singurul raspunzator pentru corectitudinea informaţiilor furnizate in vederea eliberarii certificatului. Oficiul de Stat pentru Invenţii şi Mărci este organul de specialitate al administraţiei publice centrale, unica autoritate care asigură pe teritoriul României protecţia mărcilor şi indicaţiilor geografice. In conformitate cu prevederile Legii nr. 84/1998 privind mărcile şi indicaţiile geografice, "Dreptul asupra mărcii este dobândit şi protejat prin înregistrarea acesteia la Oficiul de Stat pentru Invenţii şi Mărci." (Art. 4)."

3.2 Autentificarea identităţii Abonatului la reînnoirea sau modificarea certificatului

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

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

Identitatea Abonaților care cer reînnoirea certificatului, sau modificarea acestuia trebuie verificata.

Procedurile utilizate urmăresc verificarea faptului că persoana sau organizația care cer un nou certificat pentru un utilizator, sunt îndreptățite la acest lucru.

Abonații care trimit cereri direct la o Autoritate de Certificare pot fi verificati de această autoritate pe baza semnaturii electronice şi a certificatului cheii publice asociat cu această semnatura.

Reînnoirea sau modificarea certificatului nu se aplică pentru certificatele emise de certSIGN Clasa 1.

3.2.1 Reînnoirea unui certificat

Un Abonat sau o Autoritate de Certificare foloseşte reînnoirea dacă deține deja un certificat şi o cheie privată asociată acestuia şi doreşte să continue să folosească aceeaşi pereche de chei. Noul certificat, creat ca rezultat al înnoirii, constă în aceeaşi cheie publică, acelaşi nume şi restul informațiilor care se preiau din certificatul anterior, dar perioada de valabilitate, numărul serial şi semnatura emitentului sunt diferite față de datele din certificatul anterior. (vezi Capitolul 4.6)

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

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

3.2.2 Modificarea unui certificat

Modificarea certificatului se referă la crearea unui nou certificat pe baza certificatului deținut în prezent de Abonat. Un nou certificat are o cheie publică diferită, un nou număr serial, dar diferă prin cel puțin un câmp (prin conținut sau prin apariția unui câmp complet nou) față de certificatul pe baza căruia este emis. Modificarea poate fi necesară, de exemplu, în cazul schimbării poziției în cadrul companiei sau al schimbării numelui, cu condiția ca aceste date să fi fost menționate inițial în certificat, sau dacă trebuie adăugate. Dacă datele, verificate pe baza unor documente în concordanță cu procedurile de autentificare ale Abonatului au fost modificate, fiecare cerere

trebuie confirmată de Autoritatea de Înregistrare (vezi Capitolul 4.8). Pot fi modificate numai certificatele valide care nu au fost revocate şi al căror nume al Abonatului şi alte caracteristici nu au fost schimbate.

3.3 Autentificarea identității Abonatului la revocarea unui certificat

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

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

În ambele cazuri, trebuie să existe o identificare fără echivoc a identității Abonatului. Cererea de revocare poate să vizeze mai multe certificate. Autentificarea şi identificarea Abonatului la Autoritatea de Înregistrare se realizează ca şi la înregistrarea inițială (vezi Capitolul 3.1). Autentificarea Abonatului la Autoritatea de Certificare constă în verificarea autenticității cererii. Procedura detaliată de revocare este descrisă în Capitolul 4.9.3.

4 Cerințe operaționale

În continuare sunt prezentate procedurile de bază ale procesului de certificare. Fiecare procedură începe cu trimiterea, de către Abonat, a unei cereri: *indirect* (după confirmarea inițială a cererii de către Autoritatea de Înregistrare) sau *direct* către o Autoritate de Certificare. Pe baza cererii, Autoritatea de Certificare ia o decizie în legătură cu furnizarea / respingerea serviciului cerut. Cererile trimise trebuie să conțină informațiile necesare pentru identificarea corectă a Abonatului.

certSIGN oferă acces la următoarele servicii de bază:

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

b. revocarea certificatelor;

c. verificarea valabilității certificatelor.

Programul de lucru

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

Dacă cererea trimisă conține o cheie publică, cheia trebuie pregătită în aşa fel încât să lege criptografic cheia publică cu alte date stipulate în cerere, în special cu datele de identificare ale Abonatului. O cerere poate conține, în loc de o cheie publică, solicitarea Abonatului de a genera o cheie asimetrică în numele său. Aceasta poate fi îndeplinită de către o Autoritate de Certificare sau de Autoritatea de Înregistrare. În urma generării, cheile sunt trimise pe o cale sigură către Abonat, astfel încât cheile să nu poată fi activate de către o persoană neautorizată.

4.1 Trimiterea cererii

Cererile pentru una dintre Autoritățile de Certificare pot fi trimise direct de către un Abonat sau indirect de către un operator al Autorității de Înregistrare. Cererile Abonaților sunt trimise direct unei Autorități de Certificare sau indirect de către Autoritatea de Înregistrare. Cererile trimise

direct pot viza înregistrarea sau modificarea de certificat; alte cereri referitoare la serviciile de certificare furnizate de o Autoritate de Certificare sunt de asemenea permise.

Operatorul poate trimite către o Autoritate de Certificare cererile altor Abonaţi confirmate de operator şi în cazuri bine fondate chiar şi cereri de revocare de certificate aparţinând Abonaţilor care încalcă prezentul Cod de Practici şi Proceduri.

Cererile sunt trimise prin protocoale de comunicaţie precum HTTP, S/MIME sau TCP/IP.

certSIGN emite certificate numai pe baza cererilor de înregistrare, modificare, reînnoire sau modificare de certificate trimise de un Abonat.

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

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

4.1.1 Cererea de înregistrare

O cerere de înregistrare este trimisă de către un Abonat indirect Autorităţii de Înregistrare sau direct, unei Autorităţi de Certificare şi conţine cel puţin următoarele informaţii:

- numele complet al instituţiei sau numele şi prenumele Abonatului,
- numele distinctiv a cărui structură depinde de categoria Abonatului (vezi Capitolul 3.1.2),
- identificatori: Codul de Înregistrare al Firmei / Codul Numeric Personal

- adresa Abonatului,
- tipul de certificat cerut,
- identificatorul politicii de certificare pe baza căruia este emis certificatul,
- adresa de e-mail,
- cheia publică care va fi certificată.

Ca urmare a autentificării identității Abonatului (vezi Capitolele 3.1.8 şi 3.1.9) care cere înregistrarea şi după primirea confirmării Autorității de Înregistrare, cererea este trimisă unei Autorități de Certificare.

4.1.2 Cererea de reînnoire sau modificare certificat

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

- numele distinctiv al solicitantului (Abonatului);
- tipul de certificat pe care-l solicită Abonatul;
- identificatorul politicii de certificare pe baza căreia trebuie emis certificatul;
- cheia publică (folosită anterior în cazul înnoirii certificatului sau nouă în cazul schimbării de cheie de certificat) care va fi certificată.

4.1.3 Cererea de revocare şi suspendare certificat

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

- numele distinctiv al solicitantului (Abonatului),
- lista de certificate de revocat sau suspendat, sub forma unei perechi: numărul serial, motivul revocării.

Datele parțiale sau complete incluse în cererea de mai sus trebuie autentificate prin semnatura electronica, dacă un Abonat deține o cheie privată validă pentru crearea de semnatura.

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

În momentul suspendării certificatului, operatorii Autorității de Înregistrare şi Abonații sunt anunțați în legătură cu acest lucru.

4.2 Procesarea cererilor

certSIGN acceptă cereri înaintate individual sau colectiv. Cererile pot fi trimise *on-line* şi *off-line*.

Cererea trimisă on-line se realizează prin intermediul paginilor WWW de pe serverul certSIGN la adresa: https://www.certsign.ro. Un Abonat care vizitează site-ul respectiv completează (conform instrucțiunilor de pe site) un formular de cerere şi îl trimite unei Autorități de Certificare. Cererile pentru certificate certSIGN Class 1 sunt procesate automat, în timp ce cererile de certificate de alte nivele sunt procesate manual.

Cererea trimisă off-line se poate face:

- Prin prezentarea în persoană a Abonatului sau a reprezentantului autorizat al companiei la Autoritatea de Înregistrare sau la Autoritatea de Certificare, caz în care se completează şi se semnează de mână a cererea, se semnează contractul cu privire la prestarea serviciilor de certificare şi se generează o parola cu ajutorul căreia Abonatul va putea face managementul certificatului sau se generează un cod PIN pentru accesul securizat la dispozitivul criptografic ce conține cheile şi certificatele.
- Prin trimiterea prin poştă a cererii şi a copiilor documentelor (conform prevederilor din Tabelul 3.1.8) necesare verificării identității solicitantului; verificarea este urmată de generarea unei parole cu ajutorul căreia Abonatul va putea face managementul certificatului, sau generarea unui cod PIN pentru accesul securizat la dispozitivul criptografic ce conține cheile şi certificatele; dispozitivul criptografic este trimis înapoi solicitantului (codul PIN este trimis separat).

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

4.2.1 Procesarea cererilor la Autoritatea de Înregistrare

Fiecare cerere scrisă pe hârtie este procesată (procesarea trebuie făcută în prezența solicitantului dacă aşa este specificat în prezentul document) după cum urmează:

- operatorul Autorității de Înregistrare primeşte cererea Abonatului
- operatorul verifică datele din cerere, cum ar fi datele personale ale Abonatului (vezi procedura descrisă în Capitolul 3.1.8) şi verifică existența dovezii posesiei cheii private (vezi Capitolul 3.1.6),
- ca urmare a verificării, operatorul confirmă identitatea dintre datele declarate şi cele cuprinse în cerere; dacă cererea conține date neconforme este respinsă,
- cererea confirmată este trimisă la Autoritatea de Certificare,
- Autoritatea de Înregistrarea mai verifică şi alte date care nu sunt specificate în cerere dar sunt necesare pentru emiterea certificatului.

4.2.2 Procesarea cererilor la Autoritatea de Certificare

Autoritatea de Certificare verifică faptul că cererile au fost confirmate de către Autoritatea de Înregistrare autorizată.

4.3 Emiterea certificatelor

După primirea şi procesarea unei cereri (vezi Capitolele 4.1 şi 4.2), Autoritatea de Certificare emite un certificat. Un certificat este considerat valid (în stare activă sau pregătit) în momentul acceptării lui de către Abonat (vezi Capitolul 4.4). Perioada de valabilitate a certificatelor emise depinde de tipul de certificat şi de categoria Abonatului şi sunt în conformitate cu perioadele prezentate în Tabelul 6.3.2.2.

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

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

- dacă procedurile sunt încheiate cu succes, serverul emite un certificat şi însărcinează modulul hardware de securitate cu semnarea certificatului; certificatul este stocat în baza de date a Autorității de Certificare,
- Autoritatea de Certificare pregăteşte răspunsul conținând certificatul emis (dacă a fost emis) şi îl trimite Abonatului; certificatul nu este publicat în Depozit până la primirea confirmării Abonatului cu privire la acceptarea certificatului (vezi Capitolul 4.4).

Autoritatea de Certificare certSIGN foloseşte două metode de bază pentru anunțarea unui Abonat despre emiterea unui certificat:

- prima metodă presupune folosirea poştei sau a poştei electronice şi constă în trimiterea (la adresa furnizată de Abonat) a informațiilor ce permit Abonatului să-şi ridice certificatul. Această metodă este folosită şi când este necesară anunțarea tuturor Abonaților unei anumite Autorități de Certificare despre emiterea unei nou certificat pentru autoritatea respectivă.
- A doua metodă constă în emiterea unui certificat şi plasarea acestuia (de obicei împreună cu o cheie privată) pe un dispozitiv criptografic şi trimiterea certificatului (prin poştă) la adresa Abonatului (un cod PIN este trimis cu o scrisoare separată).

Fiecare certificat emis este publicat în Depozitul certSIGN. Publicarea certificatului este echivalenta cu notificarea altor Entități Partenere despre faptul că un certificat a fost emis pentru un Abonat. certSIGN publică un certificat în Depozit după acceptarea certificatului de către Abonat (vezi Capitolul 4.3).

4.3.1 Timpul necesar pentru emiterea unui certificat

Cererea de înregistrare şi certificare sau de reînnoire (de chei sau certificate) va fi examinata, iar Autoritatea de Certificare va emite un certificat în intervalul de timp specificat în Tabelul 4.3.1. Aceste perioade depind în primul rând de acuratețea datelor trimise în cerere şi de modul de cooperare dintre certSIGN şi solicitant.

Nivelul de credibilitate al certificatului	Perioada de aşteptare

certSIGN Clasa 1	1 zi
certSIGN Clasa 2	5 zile
certSIGN Clasa 3	5 zile
certSIGN Clasa 4	5 zile

Tabelul 4.3.1. Perioada de aşteptare maximă pentru emiterea de certificate

În cazul în care datele necesare nu sunt puse la dispoziția Autorității de Certificare în termen, sau este necesară o completare a documentației, termenul de emitere a documentației va fi prelungit.

4.3.2 Respingerea unei cereri de emitere certificat

certSIGN poate refuza emiterea unui certificat oricărui solicitant fără a-şi asuma vreo obligație sau responsabilitate pentru posibilele daune sau pierderi pe care le poate suferi Abonatul ca urmare a acestui refuz. Autoritatea de Certificare va restitui solicitantului taxa de certificat (dacă acesta a plătit-o), cu excepția cazului în care solicitantul a menționat date false în cererea sa. Refuzul emiterii de certificat poate surveni în următoarele situații:

- dacă identificatorul Abonatului (ND) coincide cu identificatorul altui Abonat,
- dacă există suspiciune sau certitudine cu privire la falsificarea sau folosirea unor date false de către Abonat,
- dacă Abonatul, într-o manieră neconvenabilă, angajează resurse şi mijloace de procesare ale certSIGN prin trimiterea unui număr de cereri în mod clar mai mare decât nevoile pe care le are acesta,
- din alte motive decât cele de mai sus.

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

4.4 Acceptarea certificatelor

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

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

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

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

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

Prin acceptarea certificatului, Abonatul acceptă regulile Codului de Practici şi Proceduri şi a Politicii de Certificare şi subscrie să respecte prevederile contractul încheiat cu certSIGN.

4.5 Folosirea certificatelor şi a cheilor

Abonaţii trebuie să folosească cheia privată şi certificatele:

- în concordanţă cu scopul lor declarat în prezentul Cod de Practici şi Proceduri şi în concordanţă cu conţinutul certificatului (câmpurile *keyUsage* şi *extendedKeyUsage*, vezi Capitolul 4.3),
- în concordanţă cu prevederile contractului dintre Abonat şi certSIGN,
- numai în perioada de valabilitate (nu se aplică certificatelor pentru verificarea semnaturii digitale),

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

Entităţile Partenere, trebuie să folosească cheile publice şi certificatele:

- în concordanţă cu scopul lor declarat în prezentul Cod de Practici şi Proceduri şi în concordanţă cu conţinutul certificatului (câmpurile *keyUsage* şi *extendedKeyUsage,* vezi Capitolul 4.3),
- în concordanţă cu prevederile contractului dintre Abonat şi certSIGN,
- numai după verificarea stării acestora (vezi Capitolul 4.9) şi verificarea semnaturii Autorităţii de Certificare care a emis acel certificat.

4.6 Re-certificarea

certSIGN oferă servicii de re-certificare a aceleiaşi perechi de chei criptografice.

4.7 Certificarea cheii

Certificarea cheii se face atunci când un Abonat (deja înregistrat) generează o nouă pereche de chei (sau comandă unei Autorităţi de Certificare să genereze o astfel de pereche de chei) şi solicită emiterea unui nou certificat care să confirme posesia cheii publice nou create. Certificarea cheii trebuie interpretate după cum urmează:

- certificarea cheii nu este asociată nici unui certificat valid şi este folosită de Abonaţi pentru a obţine unul sau mai multe certificate de orice tip, nu neapărat în cadrul aceleiaşi politici de certificare (în cazul în care clasa noului certificat este mai mică decât a certificatelor existente - de exemplu Abonatul are un certificat de clasă 3 şi solicită unul de clasă 2 - autentificarea identităţii se bazează pe aceste certificate sau pe parolele de management corespunzătoare; în caz contrar, procedurile sunt identice cu cele pentru emiterea unui nou certificat),

Certificarea cheii este realizată numai la cererea Abonatului şi trebuie precedată de înaintarea unei cereri pe formular corespunzător, completată de Abonat.

Cererile trebuie să fie confirmate în situaţia în care operatorul Autorităţii de Înregistrare solicită acest lucru.

Procedura pentru procesarea cererii de certificare a cheii este echivalenta procedurilor de procesare a cererilor de certificate descrise în Capitolul 4.2 şi procedurilor de emitere de certificate descrise în Capitolul 4.3. În urma acestui proces:

- Abonatul este notificat despre emiterea noului certificat cu noul număr serial,
- Abonatul este obligat să trimită confirmarea acceptului certificatului către o Autoritate de Certificare,
- un nou certificat este publicat în Depozitul Autorității de Certificare.

Certificarea cheii este, de asemenea, aplicabilă certificatelor unei anumite Autorități de Certificare, deşi într-un astfel de caz toți clienții Autorității de Certificare vor fi informați despre executarea procedurii.

certSIGN anunță întotdeauna Abonații (cu cel puțin 30 de zile înainte) despre apropierea momentului expirării perioadei de valabilitate. Această informație este de asemenea trimisă în cazul certificatelor Autorităților de Certificare.

4.8 Schimbarea cheii

certSIGN nu oferă servicii de schimbare a cheii unui certificat.

4.9 Modificarea certificatelor

Modificarea unui certificat presupune înlocuirea certificatului în uz (actualmente valid) cu un nou certificat în care – spre deosebire de certificatul ce va fi înlocuit – o parte din date pot fi modificate, cu excepția cheii publice.

Modificarea certificatului:

- se realizează numai la cererea Abonatului şi trebuie să se facă după înaintarea unei cereri corespunzătoare de modificare de certificat,
- poate fi executată pentru certificatele a căror perioadă de validitate nu a expirat şi care nu au fost revocate.

Numai următoarele date pot fi modificate:

- numele de familie al Abonatului (de exemplu în urma căsătoriei, divorțului etc.),

- unitatea organizațională sau postul,
- adresa e-mail,
- rolul Abonatului sau drepturile incluse în certificat,

Procedura de modificare a unui certificat necesită autentificarea cererii de către un Abonat prin semnarea electronica a acesteia. Abonatul trebuie să dețină o cheie privată valabilă pentru crearea de semnaturi electronice. Dacă Abonatul nu are o astfel de cheie, trebuie să se supună procedurilor de certificare descrise în Capitolul 4.7. Cererile de modificare a unui certificat trebuie să fie confirmate de Autoritatea de Înregistrare. Procedura de procesare a cererii de modificare a certificatului este la fel ca cea descrisă în Capitolul 4.1, iar procedura de emitere de certificat este aceeaşi cu cea descrisă în Capitolul 4.2. În urma acestui proces:

- Abonatul este notificat despre emiterea unui nou certificat cu un nou număr serial;
- Abonatul este obligat să trimită confirmarea acceptului autorizat al certificatului către o Autoritate de Certificare, în termen de 7 zile calendaristice (vezi cap 4.4);
- noul certificat este publicat în Depozitul Autorității de Certificare.

Dacă procedura de modificare este finalizată cu succes, certificatul modificat este revocat şi plasat în Lista certificatelor Revocate (CRL). Ca motiv al revocării este trecut *affiliationChanged* care semnifică: (1) că certificatul revocat a fost înlocuit cu altul, care conține date modificate, cum ar fi numele Abonatului şi (2) că Entitățile Partenere sunt informate că nu există nici un motiv să suspecteze că o cheie privată asociată certificatului a fost compromisă.

Procedura de modificare poate fi, de asemenea, aplicabilă anumitor Autorități de Certificare, şi în astfel de cazuri, toți clienții Autorității de Certificare sunt informați despre executarea procedurii.

4.10 Revocarea şi suspendarea certificatelor

Revocarea unui certificat are o influență semnificativă asupra utilizării acestuia şi asupra obligațiilor unui Abonat care deține un astfel de certificat. Imediat după după revocarea certificatului unui Abonat, certificatul trebuie considerat invalid (în stare de revocare). Similar, în cazul certificatului Autorității de Certificare – anularea validității unui certificat de acest tip

semnifică retragerea drepturilor de emitere de certificate pentru proprietarul său şi revocarea tuturor certificatelor emise de aceasta.

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

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

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

certSIGN nu oferă serviciul de suspendare a certificatelor.

4.10.1 Circumstanţele revocării unui certificat

Un exemplu de caz în care se revoca certificatul unui Abonat este pierderea controlului (sau existenţa suspiciunii acestui lucru) asupra cheii private deţinută de Abonat sau încălcarea de către Abonat a obligaţiilor/cerinţelor cuprinse în Politica de Certificare, contractului încheiat cu Autoritatea de Certificare sau Codului de Practici şi Proceduri.

Certificatul se revoca atunci când:

- informaţia conţinută de certificat s-a schimbat,
- o cheie privată, asociată unei chei publice, conţinută în certificat sau pe dispozitivul de stocare, a fost compromisă sau există un motiv serios pentru a suspecta ca a putut fi compromisă,
- părţile decid să înceteze contractul încheiat de acestea; în acest caz, revocarea este strict legată de anularea înregistrării Abonatului la Autoritatea de Certificare; dacă Abonatul însuşi nu cere revocarea, Autoritatea de Certificare sau un reprezentant al instituţiei la care este angajat Abonatul, au dreptul să o facă;
- Abonatul, deţinătorul unei chei publice, cere revocarea,

- poate fi revocat de emitent, certSIGN de exemplu, dacă un Abonat nu respectă Politica de Certificare, Codul de Practici şi Proceduri sau contractul, ori alte documente emise de Autoritatea de Certificare,
- Autoritatea de Certificare îşi încetează activitatea; în acest caz toate certificatele emise de această Autoritate de Certificare, înainte de expirarea perioadei declarate pentru oprirea serviciilor, trebuie revocate împreună cu certificatul Autorității de Certificare,
- Abonatul întârzie sau nu plăteşte plata contravaloarea serviciile prestate de către Autoritatea de Certificare,
- cheia privată sau securitatea unei Autorități de Certificare a fost compromisă intr-un mod în care pune în pericol credibilitatea certificatelor,
- Abonatul, angajat al unei organizații, nu a returnat dispozitivul criptografic folosit pentru stocarea certificatului şi a cheii private corespunzătoare, la încheierea contractului de muncă,
- în alte cazuri în care Abonatul nu se conformează regulilor acestui Cod de Practici şi Proceduri, Politicii de Certificare, sau contractului.

Cheie privată compromisă înseamnă: (1) accesul neautorizat la cheia privată sau un motiv întemeiat pe baza căruia să se suspecteze acest acces, (2) pierderea cheii private sau apariția unui motiv de a suspecta o astfel de pierdere, (3) furtul cheii private sau apariția unui motiv de a suspecta un astfel de furt, (4) ştergerea accidentală a cheii private.

Cererea de revocare poate fi trimisă (vezi Capitolul 3.4) prin intermediul Autorității de Înregistrare (aceasta implică contactarea autorității de către Abonat), sau direct unei Autorități de Certificare (cererea poate fi autentificată prin semnatura). Cererea de revocare trebuie să conțină informații care să permită autentificarea sigură a Abonatului de către Autoritatea de Înregistrare, în concordanță cu prevederile Capitolului 3.1.8, Dacă autentificarea identității Abonatului nu se realizează cu succes, Autoritatea de Certificare respinge cererea de revocare şi suspendă certificatul până când cererea de revocare va fi examinată în detaliu.

4.10.2 Cine poate cere revocarea certificatelor

Următoarele entități pot trimite cereri de revocare a certificatului unui Abonat:

- Abonatul, care este proprietarul certificatului,
- un reprezentant autorizat al Autorității de Certificare (în cazul certSIGN acest rol este rezervat administratorului de securitate),
- un mandat al Abonatului, de exemplu angajatorul sau; Abonatul trebuie imediat informat despre acest lucru,
- Autoritatea de Înregistrare care poate cere revocarea în numele unui Abonat, sau în nume propriu, dacă are informații care justifică revocarea certificatului.

Autoritatea de Înregistrare trebuie să acționeze cu multă precauție când procesează cereri ce nu au fost trimise de către un Abonat şi să accepte numai acele cereri în conformitate cu Capitolul 4.9.1.

Când partea care cere revocarea certificatului nu este proprietarul certificatului (Abonatul), Autoritatea de Certificare trebuie:

- să verifice faptul ca respectiva parte are dreptul să emita o astfel de cerere
- sa ceara o justificare a respectivei cereri
- să trimită o notificare Abonatului despre revocare, sau despre inițierea procesului de revocare.

Fiecare cerere trebuie trimisă:

- direct Autorității de Certificare sub formă electronica, cu sau fără confirmarea Autorității de Înregistrare,
- direct sau indirect (prin intermediul Autorității de Înregistrare) la Autoritatea de Certificare, sub formă ne-electronica (document pe hârtie, fax, telefon etc.)

4.10.3 Procedura de revocare a certificatelor

Revocarea certificatului se poate face în următoarele moduri:

- prima metodă se bazează pe trimiterea unei cereri de revocare în format electronic, autorizată printr-o parolă, către o Autoritate de Certificare; o astfel de revocare poate fi inițiată numai la cererea Abonatului
- a doua metodă necesită trimiterea unei cereri electronice de revocare către certSIGN , confirmată (prin semnatura electronica) de Autoritatea de Înregistrare; această metodă se aplică în situațiile în care (a) Abonatul a pierdut cheia sa privată sau parola ei, sau cheia privată a fost furată sau (b) cererea de revocare a fost trimisă de reprezentantul Abonatului, un reprezentant autorizat al unei Autorități de Certificare sau al Autorității de Înregistrare, cu condiția de a exista suficiente motive pentru a cere o astfel de revocare;
- a treia metodă implică trimiterea unei cereri ne-electronice autentificate (document pe hârtie, fax, telefon etc.) către certSIGN ; autentificarea unui document pe hârtie (inclusiv faxul) poate fi efectuată la Autoritatea de Înregistrare, de exemplu cu o ştampilă şi o semnatura de mână a unei persoane recunoscute de certSIGN, sau prin plasarea unei parole în cadrul documentului, parola cunoscută doar de persoana care cere revocarea; o cerere făcută prin telefon este îndeplinită numai după ce se trimite şi parola; după verificarea cu succes a cererii, Autoritatea de Înregistrare pregăteşte confirmarea electronica a cererii de revocare şi o înaintează Autorității de Certificare.

Informațiile despre certificatele revocate sau suspendate sunt plasate în Lista de certificate Revocate (vezi Capitolul 7.2), emisă de Autoritatea de Certificare. Autoritatea de Certificare notifică entitatea care cere revocarea certificatului despre această revocare, sau despre decizia de a anula cererea, împreună cu motivele anulării.

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

Procedura de revocare a unui certificat se desfăşoară astfel:

- Autoritatea de Certificare, ca urmare a primirii unei cereri de revocare certificat, o verifica; dacă cererea este făcută electronic, Autoritatea de Certificare verifică corectitudinea certificatului de revocat şi (opțional) corectitudinea certificatului ataşat cererii; cererea făcută pe hârtie necesită autorizarea solicitantului; o astfel de confirmare

poate fi obținută prin telefon, fax, sau în timp ce Abonatului vizitează personal un reprezentant autorizat al Autorității de Certificare (sau invers);

- dacă cererea este verificată cu succes, Autoritatea de Certificare plasează informațiile despre revocarea certificatului în Lista certificatelor Revocate (CRL), împreună cu informații privind motivele de revocare (vezi Capitolul 7.2.1);
- Autoritatea de Certificare notifică, electronic sau prin poşta, entitatea care cere revocarea despre revocare sau decizia de anulare a cererii împreună cu motivele anulării.
- în plus, dacă partea care cere revocarea nu este Abonatul, Autoritatea de Certificare trebuie să notifice Abonatul în privința revocării certificatului, sau inițierii procesului de revocare.

Dacă un certificat, sau o cheie privată corespunzătoare unui certificat de revocat au fost stocate pe un dispozitiv criptografic, ca urmare a revocării certificatului, dispozitivul criptografic trebuie distrus fizic sau şters în codiții de maximă securitate. Această operație se îndeplineşte de către posesorul dispozitivului criptografic – o persoană fizică sau juridică (un reprezentant al unei astfel de entități). Deținătorul dispozitivului criptografic trebuie să-l păstreze astfel încât să prevină furtul sau utilizarea neautorizată a sa până la distrugerea fizică sau la ştergerea cheii private.

4.10.4 Perioada maximă pentru revocarea unui certificat

certSIGN garantează următoarea perioadă maximă pentru procesarea unei cereri de revocare certificat,

- trimisă electronic (în formatul corect) sau prin telefon,
- trimisă sub formă de document din hârtie,

după cum este descris în Tabelul 4.9.4.

Politica de certificare	Perioada de grație admisibilă
certSIGN Clasa 1	Fără obligație de revocare
certSIGN Clasa 2	în 24 de ore
certSIGN Clasa 3	în 24 de ore
certSIGN Clasa 4	în 24 de ore

Tabel 4.9.4. Perioada maximă de procesare a cererii de revocare de certificat

Informațiile despre revocarea de certificat sunt stocate în baza de date a certSIGN. certificatele revocate sunt plasate în Lista certificatelor Revocate (CRL) în concordanță cu perioadele de publicare a CRL.

În momentul revocării certificatului, operatorii Autorității de Înregistrare şi Abonații implicați sunt informați automat despre această revocare. Informații despre starea curentă a certificatului sunt disponibile prin serviciul de verificare a stării certificatelor imediat după perioada de grație declarată. Acest serviciu poate fi cerut, de exemplu, de către o Entitate Parteneră, care verifică validitatea unei semnaturi electronice aplicate unui document primit de la Abonat.

4.10.5 Frecvența de emitere a CRL-urilor

Fiecare Autoritate de Certificare care face parte din certSIGN emite diferite Liste de Revocare de certificat. Un nou CRL este publicat în Depozit după fiecare revocare de certificat, într-un interval de maxim o zi. Dacă motivul revocării este compromiterea cheii, noul CRL este emis imediat după procesarea cererii de revocare (vezi Capitolul 4.9.4). Perioada de valabilitate a CRL-ului este de 48 de ore si se actualizeaza zilnic..

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

În cazul revocării certificatului unei autorități afiliate la certSIGN acest certificat este imediat publicat în Lista de certificate Revocate.

4.10.6 Verificarea Listei de Certificate Revocate

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

Verificarea stării unui certificat se poate baza în exclusivitate pe CRL numai în cazurile în care frecvența perioadelor de emitere a CRL-ului, declarata de certSIGN, nu poate aduce daune serioase sau pierderi pentru Entitatea Parteneră. În alte cazuri, o Entitate Parteneră este obligata

să contacteze (prin telefon, fax etc.) autoritatea emitentă a certificatului sau să folosească serviciul de verificare *on-line* a stării certificatelor.

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

a. *unspecified* – necunoscut
b. *keyCompromise* – compromiterea securității cheii private
c. *cACompriomise* – compromiterea securității Autorității de Certificare
d. *cessationOFOperation* – încetarea serviciilor asociate cheii private

Dacă un certificat a fost revocat din următoarele motive:

e. *affiliationChanged* – modificarea datelor,
f. *superseded* – modificarea cheii,

Decizia finală asupra credibilității certificatului se va lua de către Entitatea Parteneră. În procesul luării acestei decizii, Entitatea Parteneră trebuie să aiba în vedere faptul că motivele enuntate la punctele 4.9.6 lit f,g,h nu sunt motive să se considere că cheia privată a Abonatului a fost compromisă.

4.10.7 Verificarea on-line a stării certificatelor

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

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

- *good* – semnificând un răspuns pozitiv pentru cerere, care trebuie interpretat ca fiind confirmată validitatea certificatului,
- *revoked* – însemnând că certificatul a fost revocat,

- *unknown* – semnificând că certificatul nu a fost emis de nici una dintre Autoritățile de Certificare afiliate.

Serviciul OCSP este disponibil oricărui Abonat şi Entitate Parteneră care a semnat contractul cu certSIGN în legătură cu oferirea acestor servicii.

Starea certificatului este întotdeauna oferită în timp real (imediat după revocarea certificatului) pe baza informațiilor din baza de date a certSIGN şi conține informații mai noi decât cele din CRL-ul publicat.

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

4.10.8 Revocarea certificatului CA

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

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

4.10.9 Circumstantele suspendării unui certificat

Nu se aplică.

4.10.10 Cine poate cere suspendarea unui certificat

Nu se aplică.

4.10.11 Procedura de suspendare a unui certificat

Nu se aplică

4.10.12 Limita duratei de suspendare a unui certificat

Nu se aplică.

4.11 Managementul tokenurilor/smartcardurilor

In prezent, certSIGN nu are implementate procese de management al ciclului de viata al tokenurilor/smartcardurilor.

4.12 Înregistrarea evenimentelor şi procedurile de auditare

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

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrata şi dezvăluita atunci când se desfăşoară un audit (vezi Capitolul 2.7).

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

4.12.1 Tipuri de evenimente înregistrate

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

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

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

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

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

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

Conţinutul înregistrărilor se refera la:

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

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

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

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate, administratorilor Autorităților de Certificare şi auditorilor (vezi Capitolul 5.2).

4.12.2 Frecvența analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente trebuie revăzute în detaliu cel puțin o dată pe lună. Orice eveniment având o importanță semnificativă trebuie explicat şi descris într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări şi verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acțiune executată ca rezultat al funcționări defectuoase detectate trebuie înregistrată în jurnal.

4.12.3 Perioada de retenție a jurnalelor de evenimente

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

Jurnalele arhivate sunt păstrate cel puțin 2 ani.

4.12.4 Protecția jurnalelor de evenimente

Săptămânal, fiecare înregistrare din jurnale face obiectul arhivării pe bandă magnetică. După depăşirea numărului acceptat de înregistrări pentru un jurnal, conținutul acestuia este arhivat. Arhivele pot fi criptate folosind algoritmul Triple DES sau AES. O cheie folosită pentru criptarea arhivelor este plasată sub controlul administratorului de securitate.

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

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

În plus, procedurile de protecție a jurnalului sunt implementate în aşa fel încât, chiar şi după arhivarea jurnalului, este imposibil să ştergi înregistrări, sau să ştergi jurnalul înaintea expirării perioadei de retenție a jurnalului (Vezi Capitolul 4.10.3).

4.12.5 Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate certSIGN solicita ca jurnalul de evenimente să facă obiectul backup-ului lunar. Aceste backup-uri sunt stocate în locații auxiliare ale certSIGN.

4.12.6 Notificarea entităților responsabile de tratarea evenimentelor

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

4.12.7 Analiza vulnerabilităților

Autoritățile de Certificare, Autoritatea de Înregistrare şi Depozitul sunt obligate să facă o analiză a vulnerabilităților pentru fiecare procedură internă, aplicație şi sistem informatic. Cerințele de analiză pot, de asemenea, să fie stabilite de către o instituție externă, autorizată să auditeze certSIGN. Administratorul de securitate are sarcina de a efectua audituri interne prin care să verifice conformitatea înregistrărilor din jurnalul de securitate, corectitudinea copiilor de backup, activitățile executate în cazul apariției unei amenințări şi conformitatea cu Codul de Practici şi Proceduri.

Instituția externă care efectuează auditul de securitate, trebuie să desfăşoare această activitate respectând recomandările ISO/IEC 13335 (Guidelines for Management of IT Security) şi ISO/IEC 17799 (Code of Practice for Information Security Management).

4.13 Procedura de backup si restaurare

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

- discurile de instalare a aplicațiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicațiilor pentru Autoritățile de Certificare şi Înregistrare.
- serverul Web şi discurile pentru instalarea Depozitului,
- istoricul cheilor, certificatelor şi CRL-urilor autorităților,
- datele din Depozit,
- datele privind Abonații şi personalul certSIGN,
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influență deosebită asupra timpului şi costului restaurării Autorității de Certificare după defectarea, sau distrugerea sistemului. certSIGN foloseşte atât backup-uri full (săptămânale), cat şi backup-uri incrementale (zilnice), toate copiile

sunt clonate şi clonele sunt păstrate în altă locaţie, în aceleaşi condiţii de securitate ca şi cele din locaţia primară.

Procedura de restaurare va fi verificata cel puţin o data la 3 luni, pentru a se verifica utilitatea backup-ului, in caz de crash. Va trebui sa se verifice daca datele salvate pe banda sunt suficiente pentru restaurarea sistemului in cel mai scurt timp posibil. Concluziile testelor vor fi inregistrate.

4.14 Arhivarea înregistrărilor

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

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

Arhivele off-line conţin certificate (inclusiv certificatele revocate) expirate cu până la 10 ani înainte de data curentă. Arhiva certificatelor revocate conţine informaţii despre certificatul identificat, motivul revocării, dacă şi când a fost certificatul plasat în CRL. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente vechi, semnate electronic de un Abonat.

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

4.14.1 Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informaţiile rezultate în urma examinării şi evaluării (ca urmare a unui audit) măsurilor de protecţie logice şi fizice ale unei Autorităţi de Certificare, Autorităţii de Înregistrare şi Depozitului,

- cererile primite şi deciziile emise, în formă electronica, trimise de, sau către un Abonat sub formă de fişiere sau mesaje electronice,
- baza de date cu Abonați,
- baza de date cu certificate,
- Listele de certificate Revocate emise,
- istoria cheii Autorității de Certificare, de la generare până la distrugere,
- istoria cheilor Abonaților, de la generare până la distrugere, dacă cheia se arhivează în baza de date a Autorității de Certificare,
- .

4.14.2 Frecvența arhivării datelor

Arhivarea datelor se realizează pe mai multe nivele, astfel:

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

4.14.3 Perioada de păstrare a arhivelor

Datele arhivate (sub formă electronica sau pe hârtie), descrise în Capitolul 4.12 sunt păstrate pentru perioada de timp prezentată în Tabelul 4.4. După expirarea perioadei de păstrare declarate, datele arhivate sunt distruse.

Politica de certificare	Perioada minimă de păstrare a arhivelor
certSIGN Clasa 2	15 ani
certSIGN Clasa 3	15 ani
certSIGN Clasa 4	15 ani

Tabelul 4.4. Perioadele minime de păstrare a arhivelor

4.14.4 Cerințele pentru marcarea temporala a înregistrărilor

Se recomandă ca datele arhivate să fie semnate cu o marcă temporala, creată de Autoritatea de Marcare Temporala (TSA) autorizată, având certificatul emis de Autoritatea de Certificare operațională afiliată la certSIGN CA. Serviciul de marcare temporala este disponibil în cadrul certSIGN .

4.14.5 Procedurile de acces şi verificarea informațiilor arhivate

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

4.15 Schimbarea cheii unei Autorități de Certificare

Procedurile de schimbare a cheii (key changeover) se aplică cheilor Autorităților de Certificare afiliate la certSIGN şi descriu modul în care se face schimbarea cheilor certificatelor

autorităţilor, folosite pentru semnarea certificatelor utilizatorilor sau CRL-urilor. Procedura de schimbare a cheii se bazează pe emiterea de către Autoritatea de Certificare a unui certificat special, ce permite unui Abonat care deţine vechiul certificat al autorităţii să-l obţină pe cel nou iar noilor Abonaţi care au deja noul certificat al autorităţii să-l obţină pe cel vechi pentru verificarea datelor curente. Fiecare schimbare de cheie a Autorităţii de Certificare este anunţată în avans prin intermediul paginilor de Web ale certSIGN şi difuzată prin poşta electronica către fiecare Abonat al Autorităţii de Certificare a cărei chei urmează a fi schimbate. În plus, în cazul schimbării cheii certSIGN ROOT CA, informaţiile despre acest eveniment vor fi publicate prin intermediul mass-media cu o luna înainte de momentului expirării perioadei de valabilitatea a cheii private. Frecvenţa schimbării cheilor unei Autorităţi de Certificare afiliată la certSIGN este dată de perioada de valabilitate a certificatului autorităţii, după cum este prezentat în Tabelul 6.3.2.1

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

4.16 Compromiterea securităţii cheii şi recuperarea în caz de dezastru

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

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

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

- distrugerea fizică a sistemului de calcul al certSIGN, inclusiv a resurselor de reţea – această ameninţare se referă la distrugerile provocate de situaţiile de urgenţă,
- funcţionarea defectuoasă a aplicaţiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicaţiile utilizatorilor şi executarea de aplicaţii periculoase, cum ar fi viruşii, viermii, caii troieni,
- pierderea unor servicii de reţea importante pentru activitatea certSIGN . Acestea se referă în primul rând la căderile de tensiune şi distrugerea legăturilor de reţea.

- distrugerea unei părți din Intranetul folosit de certSIGN pentru a furniza servicii – acest lucru poate duce la obstrucționarea clienților şi refuzul (neintenționat) serviciilor.

Pentru a preveni sau limita efectele amenințărilor de mai sus:

- Politica de securitate a certSIGN include un Plan de continuitate a afacerii şi recuperare în caz de dezastru,
- În cazul apariției unui eveniment ce blochează funcționarea certSIGN, în maxim 48 de ore, va fi activată locația auxiliară ce poate substitui toate funcțiile importante ale unei Autorității de Certificare până la restaurarea locației principale. 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 aplicațiilor software în producție se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al certSIGN.
- Sistemul certSIGN dispune de aplicații pentru crearea copiilor de backup pe baza cărora se poate face în orice moment restaurarea sistemului şi auditarea acestuia. Copiile de siguranță includ toate datele relevante din punct de vedere al securității.

4.16.2 Compromiterea sau suspiciunea compromiterii cheii private a unei Autorități de certificare

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

- Autoritatea de Certificare generează o nouă pereche de chei şi un nou certificat,
- toți utilizatorii de certificate sunt informați imediat despre compromiterea cheii private prin intermediul mass-media sau poştei electronice,
- certificatul corespunzător cheii compromise va fi pus în Lista de certificate Revocate,
- toate certificatele din calea de certificare a certificatului compromis sunt revocate, specificându-se motivul revocării,

- se generează noi certificate pentru Abonaţi,
- noile certificate sunt trimise Abonaţilor în mod gratuit.

4.16.3 Coerenţa securităţii după dezastru

După fiecare recuperare a sistemului ca urmare a unui dezastru, administratorul de securitate sau administratorul Autorităţii de Certificare trebuie să acţioneze în conformitate cu Planul de continuitate a afacerii şi recuperare în caz de dezastru.

4.17 Încetarea activităţii unei Autorităţii de Certificare sau transferarea serviciilor

Obligaţiile prezentate mai jos sunt stabilite pentru a minimiza efectele negative asupra Abonaţilor şi Entităţilor Partenere, ce pot apare ca urmare a deciziei unei Autorităţi de Certificare de a-şi înceta activitatea şi se refera la obligaţiile de a notifica în prealabil toţi Abonaţii autorităţii care a certificat Autoritatea de Certificare care-şi încetează activitatea (dacă există o asemenea autoritate) şi transferarea responsabilităţilor (servicii oferite Abonaţilor, baza de date, etc.), conform reglementărilor în vigoare, unei alte Autorităţi de Certificare.

4.17.1 Cerinţe specifice transferului responsabilităţii

Înainte ca o Autoritate de Certificare să-şi înceteze activitatea, este obligată să:

- anunţe Autoritatea de Certificare care a emis certificatul său despre intenţia de a-şi înceta activitatea ca Autoritate de Certificare autorizată; notificarea trebuie făcută cu 90 de zile înainte de data stabilită pentru încetarea efectivă a activităţii,
- să anunţe (cu cel puţin 30 de zile înainte) Abonaţii săi care au certificate active (neexpirate şi nerevocate) emise de autoritatea respectivă despre decizia de a-şi înceta activitatea,
- să revoce toate certificatele care rămân active (neexpirate şi nerevocate) în momentul declarat al încetării activităţii, indiferent dacă Abonatul a trimis sau nu o cerere în acest sens,
- să anunţe toţi Abonaţii Autorităţii de Certificare despre încetarea activităţii,

- să depună toate eforturile pentru a minimiza efectele negative asupra intereselor Abonaților şi persoanelor juridice angajate în procese de verificare a semnaturilor electronice folosind certificate digitale emise de Autoritatea de Certificare care îşi încheie activitatea,
- să propună încheierea unui contract (de exemplu cu o altă Autoritate de Certificare, conform Capitolului 4.14.2) prin care să se garanteze protecția datelor,
- să plătească compensații (care să nu depăşească taxele de emitere şi depozitare a certificatelor) Abonaților al căror certificat neexpirat şi nerevocat va fi revocat înainte de data expirării.

4.17.2 Emiterea certificatelor de către succesorul Autorității de Certificare care îşi încetează activitatea

Pentru a asigura continuitatea serviciilor de emitere certificate pentru Abonați, Autoritatea de Certificare care îşi încetează activitatea poate semna un contract cu o altă Autoritate de Certificare ce oferă servicii similare, pentru a emite certificate care să înlocuiască certificatele rămase în uz, emise de Autoritatea de Certificare care îşi încheie activitatea.

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

Arhiva Autorității de Certificare care-şi încetează activitatea trebuie predată Autorității de Certificare primară, certSIGN ROOT CA (în cazul încetării activității autorități certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3 şi certSIGN Non-Repudiation CA Class 4) sau instituției cu care s-a semnat contractul (în cazul sistării activității autorități certSIGN ROOT CA).

5 Controale de securitate fizică, organizațională şi de personal

Acest capitol descrie cerințele generale privind securitatea fizică şi organizațională, precum şi activitatea personalului certSIGN în activitatea de generare de chei, verificarea autenticității entităților, emiterea şi publicarea certificatelor, revocarea certificatelor, audit şi crearea de copii de siguranță.

5.1 Controale de securitate fizică

5.1.1 Controale de securitate fizică în cadrul certSIGN

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

5.1.1.1 Amplasarea locației

certSIGN este localizată în Bucureşti, la următoarea adresă: Sos Oltenitei 107A, C1, parter

5.1.1.2 Accesul fizic

Accesul fizic în cadrul certSIGN este controlat şi monitorizat de un sistem de alarmă integrat. certSIGN dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruşilor şi sisteme de alimentare cu energie electrică în caz de urgență.

Sediul certSIGN şi Autoritatea de Certificare sunt accesibile publicului în fiecare zi lucrătoare între 10:00 şi 16:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea certSIGN. Vizitatorii locațiilor aparținând certSIGN trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de certSIGN se împart în:

- zona serverelor,

- zona operatorilor CA
- zona operatorilor RA şi administratorilor,
- zona de dezvoltare şi testare.

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

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

Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. În această zonă este permisă şi prezenţa persoanelor neînsoţite. Programatorii şi dezvoltatorii nu au acces la informaţii senzitive. Dacă este necesar un astfel de acces, atunci el se poate face numai în prezenţa administratorul de securitate. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de dezvoltare al certSIGN.

5.1.1.3 Sursa de alimentare cu electricitate şi aerul condiţionat

Zona operatorilor şi administratorilor, precum şi zona de dezvoltare şi testare sunt prevăzute cu aer condiţionat. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii.

5.1.1.4 Expunerea la apă

Riscul de inundaţie în zona serverelor este mic datorita faptului ca distanta fata de sol este de cca 1m.

5.1.1.5 Prevenirea incendiilor

Locația certSIGN dispune de sistem de prevenire şi protecție împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

5.1.1.6 Depozitarea mediilor de stocare a informațiilor

În funcție de sensibilitatea informațiilor, mediile electronice care conțin arhivele şi copiile de siguranță ale datelor curente sunt stocate în seifuri metalice, localizate într-o camera cu grad ridicat de securitate. Accesul la camera şi seifuri este permis numai persoanelor autorizate.

5.1.1.7 Aruncarea deşeurilor

Hârtiile şi mediile electronice care conțin informații importante din punct de vedere al securității certSIGN sunt distruse după expirarea perioadei de păstrare (vezi Capitolul 4.12). Modulele de securitate hardware sunt resetate şi şterse conform recomandărilor producătorului. Aceste dispozitive sunt, de asemenea, resetate şi şterse atunci când sunt trimise în service sau reparate.

5.1.1.8 Depozitarea backup-urilor în afara locației

Copiile parolelor, codurile PIN şi cardurile criptografice sunt stocate în containere speciale, situate în afara locației certSIGN.

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

5.1.2 Controale de securitate fizică în cadrul Autorității de Înregistrare

Calculatoarele folosite pentru înregistrarea cererilor Abonaților şi emiterea confirmărilor trebuie amplasate în zone special amenajate şi trebuie să opereze în mod on-line (să fie conectate la rețea). Aceste calculatoare sunt protejate fizic împotriva accesului persoanelor neautorizate.

5.1.2.1 Amplasarea locației

Autoritatea de Înregistrare (RA) este amplasată în zona operatorilor şi administratorilor din cadrul certSIGN. (vezi Capitolul 5.1.1.2),

5.1.2.2 Accesul fizic

Accesul la Autoritatea de Înregistrare se desfăşoară în aceleaşi condiţii cu cele descrise în Capitolul 5.1.1.2.. Accesul trebuie monitorizat şi permis numai persoanelor autorizate din cadrul Autorităţii de Înregistrare (operatorii Autorităţii de Înregistrare, administratorii etc.) şi clienţilor acesteia.

5.1.2.3 Sursa de alimentare cu electricitate şi aerul condiţionat

Clădirea Autorităţii de Înregistrare trebuie dotată cu sisteme de alimentare electrică de urgenţă (UPS), care să permită continuarea lucrului timp de câteva minute din momentul căderii tensiunii. Aerul condiţionat nu este necesar.

5.1.2.4 Expunerea la apă

Acest Cod de Practici şi Proceduri nu specifică nici un fel de condiţii în această privinţă, pentru Autoritatea de Înregistrare.

5.1.2.5 Prevenirea şi protecţia împotriva incendiilor

Acest Cod de Practici şi Proceduri nu specifică nici un fel de condiţii în această privinţă, pentru Autoritatea de Înregistrare.

5.1.2.6 Depozitarea mediilor electronice

Mediile folosite pentru stocarea arhivelor şi a copiilor de siguranţă ale datelor curente sunt păstrate în seifurile Autorităţii de Certificare.

5.1.2.7 Aruncarea deşeurilor

Hârtiile şi mediile electronice care conţin date confidenţiale sau secrete sunt distruse după expirarea perioadei de păstrare (vezi Capitolul 4.12).

5.1.2.8 Depozitarea arhivelor în afara locaţiei

Stocarea arhivelor şi a copiilor de siguranţă ale datelor curente trebuie să se facă în afara locaţiei Autorităţii de Înregistrare.

5.1.2.9 Depozitarea copiilor de backup de urgență

Datele arhivate, copiile de siguranță de urgență şi alte informații senzitive sunt păstrate în seifuri, accesibile exclusiv angajaților autorizați ai certSIGN.

5.1.3 Securitatea fizică a Abonatului

Abonații trebuie să-şi protejeze parola de acces la sistem şi PIN-ul. Posesorii de certificate nu trebuie să-şi lase stația de lucru nesupravegheată atunci când aceasta se află într-o stare nesigură din punct de vedere criptografic, de exemplu, după ce au introdus parola sau PIN-ul ce activează cheia privată.

În cazul unei chei private stocate (după criptarea acesteia cu parola Abonatului) pe un mediu nesecurizat, de exemplu, o dischetă, mediul respectiv trebuie protejat împotriva accesului neautorizat.

5.2 Controlul securității organizației

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparținând certSIGN, Autorității de Înregistrare şi instituțiilor Abonate. De asemenea, tot în acest capitol sunt descrise responsabilitățile şi sarcinile specifice fiecărui rol.

5.2.1 Roluri de încredere

5.2.1.1 Roluri de încredere în certSIGN

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

- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate. În plus poate aproba/revoca/suspenda certificate.
    - Inițiază instalarea, configurarea şi managementul aplicațiilor software şi hardware (inclusiv resursele de rețea) ale certSIGN; inițiază şi suspendă serviciile oferite de certSIGN; coordonează administratorii, inițiază şi supraveghează generarea de chei şi secrete partajate; atribuie drepturi din punct de vedere al securității şi privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile

utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne şi externe; primeşte şi răspunde la rapoartele de audit; supervizează eliminarea deficienţelor constatate în urma auditului.

- Supraveghează operatorii Autorităţii de Certificare; configurează sistemele şi reţeaua, activează şi configurează mecanismele de protecţie a reţelei; creează conturile pentru utilizatorii certSIGN; verifică log-urile de sistem; verifică respectarea Politicii de certificare şi a Codului de Practici şi Proceduri; generează secrete partajate şi chei; administrează Lista de certificate Revocate; creează copiile de siguranţă de urgenţă; modifică numele şi adresele serverelor.

- **Administratorul de sistem** – Autorizat să instaleze, configureze şi să întreţină sistemele de încredere ale Autorităţii de Certificare pentru înregistrarea, generarea de certificate, iniţializarea dispozitivelor şi gestiunea revocărilor de certificate. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **Operatorul de sistem** – Responsabil de operarea zilnică a sistemelor de încredere ale Autorităţii de Certificare. Autorizat să execute operaţiile de backup şi restaurare a sistemului. Are acces la certificatele Abonaţilor; revocă certificatele Abonaţilor; asigură continuitatea copiilor de siguranţă şi arhivelor bazelor de date şi a creării log-urilor de sistem; administrează bazele de date; are acces la informaţii confidenţiale despre Abonaţi, dar nu poate accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranţă ale arhivei şi ale datelor curente în afara locaţiei certSIGN.
- **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale Autorităţii de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi Proceduri de către Autoritatea de Certificare; această responsabilitate se extinde şi asupra Autorităţii de Înregistrare care operează în cadrul certSIGN.
- **Administratorul depozitului** – administrează directoarele certSIGN disponibile publicului, creează şi actualizează conţinutul directoarelor din depozit, creează paginile Web şi administrează legăturile (link-urile).

*În cadrul certSIGN, rolul de **auditor** nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.*

5.2.1.2 Roluri de încredere în Autoritatea de Înregistrare

certSIGN trebuie să se asigure că personalul Autorității de Înregistrare este conştient de responsabilitățile pe care le are cu privire la verificarea informațiilor despre Abonați. Prin urmare, în cadrul unei Autorități de Înregistrare trebuie definite cel puțin următoarele 3 roluri de încredere:

- **Administratorul de sistem** – instalează dispozitivele hardware şi sistemele de operare; instalează programe; configurează sistemul şi aplicațiile; activează şi configurează resursele de securitate; creează conturi şi parole pentru operatori; creează copii de siguranță şi arhivează datele; verifică jurnalele de evenimente (log-uri) şi (împreună cu operatorul Autorității de Înregistrare), la ordinul administratorului de secrete, şterge datele în exces.
- **Administratorul de secrete** – supervizează şi transferă secretele (cheile criptografice şi alte date protejate) către operatorii Autorității de Înregistrare; ia parte la activarea modulului criptografic şi la încărcarea cheilor operatorilor (în prezența acestora); transferă şi activează cardurile de identitate ale operatorilor (dacă aceste carduri sunt blocate); mediază contactele dintre Autoritatea de Înregistrare şi Autoritatea de Certificare;
- **Operatorii** – verifică identitatea Abonaților şi corectitudinea cererilor primite; emit confirmări ale cererilor pe care le trimit Autorității de Certificare; generează cheile şi iau parte la generarea certificatelor, trimițând informațiile din cerere la o Autoritate de Certificare; arhivează (sub formă de documente pe hârtie) cererile şi confirmările emise, care fac obiectul ştergerii, la ordinul administratorului de secrete şi în prezența acestuia,

5.2.1.3 Funcțiile de încredere ale Abonaților

Abonatul poate nominaliza o persoană (operator) care să exploateze aplicațiile pentru schimbul electronic de date. Persoana respectivă este răspunzătoare de semnarea, criptarea şi transmiterea mesajelor.

5.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini

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

Prezenţa administratorului de securitate, a administratorului Autorităţii de Certificare şi a unui număr corespunzător de posesori de secrete partajate este necesară şi la încărcarea cheii criptografice a Autorităţii de Certificare în modulul hardware de securitate. Încărcarea cheii criptografice a Autorităţii de Înregistrare în modulul hardware de securitate (daca este cazul) necesită prezenţa administratorului de secrete şi a unui operator al Autorităţii de Înregistrare.

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

5.2.3 Identificarea şi autentificarea pentru fiecare rol

Personalul certSIGN este supus identificării şi autentificării în următoarele situaţii:

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

Fiecare cont asignat:

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

Operațiile efectuate în certSIGN care necesită acces la resurse de rețea comune sunt protejate prin mecanisme de autentificare sigură şi de criptare a informațiilor transmise.

5.3 Controlul personalului

certSIGN trebuie să se asigure că persoana care îndeplineşte responsabilitățile funcției, conform cu rolul atribuit în cadrul unei Autorități de Certificare sau Înregistrare:

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

5.3.1 Experiența personală, calificările şi clauzele de confidențialitate necesare

Personalul angajat al certSIGN care îndeplineşte un rol de încredere, trebuie să obțină avizul responsabilului de securitate. Avizul nu este necesar în cazul persoanelor care nu exercită un rol de încredere.

Întreg personalul angajat care îndeplineşte funcții ce necesită acces la informații clasificate este autorizat în acest sens de către ORNISS (Oficiul Registrului Național al Informațiilor Secrete de Stat).

Îndeplinirea unei funcții de încredere ca administrator de securitate, administrator al Autorității de Certificare şi administrator de secrete (din cadrul Autorității de Înregistrare) permite accesul

la informațiile clasificate. Dezvăluirea neautorizată a acestor informații poate cauza pierderea sau compromiterea intereselor, apărate de lege, ale unei persoane fizice sau ale unei organizații.

Procedurile de acces la informațiile nepublice şi de verificare a încrederii în personal sunt în conformitate cu Legea Protecției Datelor cu Caracter Personal.

5.3.2 Cerințele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a angajării la certSIGN, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici şi Proceduri,
- reglementările Politicii de certificare,
- procedurile şi controalele de securitate folosite de Autoritatea de Certificare şi Autoritatea de Înregistrare,
- aplicațiile software ale Autorității de Certificare şi Autorității de Înregistrare,
- responsabilitățile ce decurg din rolurile şi sarcinile executate în sistem,
- procedurile ce trebuie executate ca urmare a apariției unei defecțiuni în funcționarea sistemului Autorității de Certificare.

După încheierea pregătirii, participanții semnează un document prin care confirmă familiarizarea lor cu Codul de Practici şi Proceduri, Politica de certificare şi acceptă restricțiile şi obligațiile impuse.

5.3.3 Frecvența stagiilor de pregătire

Pregătirea descrisă în Capitolul 5.3.2 trebuie repetată de fiecare dată când apar modificări semnificative în certSIGN sau la Autoritatea de Înregistrare.

5.3.4 Rotația funcțiilor

Acest Cod de Practici şi Proceduri nu specifică nici un fel de cerințe în această privință.

5.3.5 Sancționarea acțiunilor neautorizate

În cazul descoperirii sau existenței suspiciunii unui acces neautorizat, administratorul de sistem împreună cu administratorul de securitate (în cazul angajaților certSIGN) poate suspenda accesul

persoanei respective la sistemul certSIGN. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare şi trebuie să fie conforme cu prevederile legale.

5.3.6 Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) face obiectul unor verificări similare ca şi în cazul angajaților certSIGN (vezi Capitolul 5.3.1, 5.3.2 şi 5.3.3). În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară activitatea în locația certSIGN, trebuie permanent însoțit de către un angajat al certSIGN , cu excepția celor care au primit avizare din partea administratorului de securitate şi care poate accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

5.3.7 Documentația oferită personalului

certSIGN trebuie să ofere personalului său accesul la următoarele documente:

- Politica de certificare,
- Codul de Practici şi Proceduri,
- Responsabilitățile şi obligațiile asociate rolului deținut în sistem.

6 Controale tehnice de securitate a informației

Acest capitolul descrie procedurile de generare şi management a perechii de chei criptografice a Autorității de Certificare şi Abonatului, inclusiv cerințele tehnice asociate.

6.1 Generarea şi folosirea perechii de chei

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

Autoritatea de Certificare **certSIGN ROOT CA** deține cel puțin un certificat autosemnat. Cheia privată corespunzătoare cheii publice conținută de certificatul autosemnat este folosită exclusiv în scopul semnării cheilor publice ale Autorităților de Certificare **certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Enterprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4**, prin semnarea certificatelor operaționale şi a Listei de certificate Revocate, necesare pentru funcționarea autorităților respective. Un rol similar îl au cheile private deținute de fiecare autoritate: **certSIGN Demo CA Class 1, certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Entreprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4** corespunzătoare cheilor publice incluse în certificatele emise de **certSIGN ROOT CA** pentru fiecare autoritate.

Perechile de chei deținute de fiecare Autoritate de Certificare trebuie să permită semnarea de certificate şi CRL - o cheie publică asociată cu o cheie privată autentificată cu un certificat autosemnat (în cazul **certSIGN ROOT CA**) sau certificat (în cazul **certSIGN Demo CA Class 1, certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Entreprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4**).

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

6.1.1 Generarea perechilor de chei

Cheile **certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3, certSIGN Non-Repudiation CA Class 4** precum şi ale altor autorităţi subordonate sunt generate în cadrul locaţiei certSIGN, în prezenţa unui grup de persoane de încredere (administratorul de securitate şi administratorul Autorităţii de Certificare sunt membri ai acestui grup).

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

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

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

În general, fiecare Abonat îşi generează singur perechea de chei. Pentru aceasta se va folosi de aplicaţia disponibila pe site-ul web al certSIGN, în momentul creării cererii. Aplicaţia permite crearea cheilor atât pe dispozitive securizate (tokenuri, smart carduri), cat şi în format p12 criptat. Generarea poate fi, de asemenea, făcută de către o Autoritate de Certificare.

certSIGN poate, la cererea Abonatului sau la cererea operatorului Autorităţii de Certificare, să genereze o pereche de chei şi să o trimită în siguranţă Abonatului. În astfel de cazuri sunt folosite aplicaţii şi dispozitive criptografice conforme cu FIPS 140-2 Nivel 2 (vezi Capitolul 6.1.2).

6.1.1.1 Procedurile de generare a cheilor inițiale ale certSIGN ROOT CA

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

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

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

6.1.1.2 Procedurile de generare a cheilor inițiale ale certSIGN CA

Procedurile de generare a cheilor inițiale pentru certSIGN CA includ:

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

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

6.1.1.3 Procedura de schimbare a cheii certificatului pentru certSIGN ROOT CA

Cheile criptografice ale certSIGN ROOT CA au o perioadă de viață limitată; dacă această perioadă a expirat, cheile trebuie actualizate.

Actualizarea perechii de chei folosite pentru semnarea de certificate şi CRL-uri se face folosind o procedură specifică. Aceasta se bazează pe emiterea de certificate speciale de către certSIGN ROOT CA. certificatele dau posibilitatea Abonaților care au instalat deja un certificat expirat al certSIGN ROOT CA să treacă în siguranță la utilizarea noului certificat; noii Abonați care posedă deja noul certificat pot să obțină în siguranță certificatul expirat, care poate fi necesar la verificarea datelor semnate în trecut.

Pentru a obține efectul descris mai sus, certSIGN ROOT CA aplică o procedură prin intermediul căreia generarea unei noi perechi de chei va permite autentificarea noii chei publice prin folosirea cheii private vechi şi invers (o cheie publică veche este autentificată cu o cheie privată nouă). Aceasta înseamnă că, drept rezultat al actualizării certificatului Autorității de Certificare, certSIGN ROOT CA, în afară de certificatul nou, mai sunt create încă două certificate. După actualizarea cheii, sunt create patru certificate pentru semnarea de certificate şi CRL-uri: certificatul vechi **OldWithOld** (cheia publică veche este semnată cu cheia privată veche), certificatul nou **NewWithNew** (cheia publică nouă este semnată cu cheia privată nouă), certificatul **OldWithNew** (cheia publică veche este semnată cu cheia privată noua) şi certificatul **NewWithOld** (cheia publică nouă este semnată cu cheia privată veche).

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

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

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

Vechea cheie publică (vechiul certificat) este disponibilă publicului până când toți Abonații obțin noul certificat (noua cheie publică) a certSIGN ROOT CA (acesta trebuie obținută înaintea datei de expirare a vechiului certificat).

Începutul şi expirarea perioadei de validitate a certificatului **OldWithNew** ar trebui să fie aceeaşi cu data de început şi de expirare a certificatului vechi.

Perioada de validitate a certificatului **NewWithOld** începe din momentul generării noii perechi de chei şi expiră în momentul în care toți Abonații vor obține noile certificate (certificatul noii chei publice) ale certSIGN ROOT CA. Momentul expirării nu ar trebui să fie mai mare decât cel al expirării vechiului certificat.

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

6.1.1.4 Procedura de schimbare a cheii certificatelor autorităților subordonate

Procedura de schimbare (actualizare) a cheii Autorității de Certificare pentru **certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4** se desfăşoară în mod similar cu cea pentru **certSIGN ROOT CA** (vezi Capitolul 6.1.1.3) cu excepția unui singur pas: certificatul **NewWithNew** este emis de către autoritatea superioară.

6.1.2 Distribuirea cheii private către entități

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

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

certSIGN garantează că după generarea perechii de chei la cererea unui Abonat, cheile nu vor fi folosite pentru crearea de semnaturi electronice şi că Autoritatea de Certificare nu va crea

condiţii pentru crearea de semnaturi de către nici o entitate neautorizată, cu excepţia proprietarului cheii private.

6.1.3 Distribuirea cheii publice către Autoritatea de Certificare

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

Cererile trimise unei Autorităţi de Certificare pot necesita, în anumite cazuri, o confirmare emisă de Autoritatea de Înregistrare (vezi Capitolele 3 şi 4).

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

6.1.4 Distribuirea cheii publice a Autorităţii de Certificare către Entităţile Partenere

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

Autorităţile de Certificare certSIGN distribuie certificatele proprii în două moduri diferite:

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

In cazul schimbării (actualizării) cheii Autorităţii de Certificare certSIGN-ROOT CA, depozitul trebuie să conţină toate certificatele autosemnate sau certificatele emise ca urmare a execuţiei procedurii descrise în Capitolul 6.1.1.3.

6.1.5 Dimensiunea cheilor

Dimensiunea cheilor folosite de Autorităţile de Certificare, operatorii Autorităţii de Înregistrare şi Abonaţi sunt prezentate în Tabelul 6.1.

Proprietarul cheii	Folosirea principală a cheii		
	RSA pentru semnarea de certificat şi CRL	RSA pentru semnarea de mesaje	RSA pentru schimbul de chei
certSIGN ROOT CA	2048 biți	-	-
certSIGN CA	2048 biți	-	-
certSIGN Demo CA Clasa 1	2048 biți	-	-
certSIGN CA Clasa 2	2048 biți	-	-
certSIGN Qualified CA Clasa 3	2048 biți	-	-
certSIGN Enterprise CA Clasa 3	2048 biți	-	-
certSIGN Non-Repudiation CA Clasa 4	2048 biți	-	-
Operatorul Autorității de Înregistrare	-	1024 biți	-
Persoane fizice şi dispozitivele hardware ale acestora	-	1024 biți	1024 biți
Persoane juridice şi dispozitivele hardware ale acestora	-	1024 biți	1024 biți

Tabel 6.1. Dimensiunea cheilor folosite

6.1.6 Parametrii de generare a cheilor publice şi verificarea calității parametrilor

Cel care generează o cheie este responsabil de verificarea calității parametrilor cheii generate. Acesta trebuie să verifice:

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

6.1.7 Generarea de chei hardware şi/sau software

Metodele permise pentru generarea de chei depind de Politica de certificare aplicată şi sunt prezentate în Tabelul 6.2. În cazul Autorităților de Certificare, cheile sunt generate prin intermediul modulelor hardware de securitate care respectă prevederile prezentate în Capitolul 6.2.1. Cheile operatorilor Autorității de Înregistrare sunt generate utilizând module hardware de securitate care îndeplinesc standarde de nivel mai scăzut (decât cel descris în Capitolul 6.2.1.). În cazul generării cheii de către un Abonat, Autoritatea de Certificare acceptă atât metode de generare hardware cât şi software (Capitolul 6.2.1).

Politica de certificare	Metoda de generare de cheie	Observații
certSIGN Clasa 1	Hardware sau software	

certSIGN Clasa 2	Hardware sau software	
certSIGN Clasa 3	Hardware	Cu excepția severelor de web şi VPN, caz în care cheile sunt generate de abonat
certSIGN Clasa 4	Hardware	

Tabelul 6.2. Metoda de generare a cheii Abonatului

6.1.8 Folosirea cheilor

Scopurile în care pot fi folosite cheile sunt date de câmpul **KeyUsage** (vezi Capitolul 7.1.1.2) din cadrul extensiilor standard ale certificatelor X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de aplicația Abonatului care face managementul certificatelor.

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

a) **digitalSIGNature**: certificat pentru verificarea de semnaturi electronice

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

c) **keyEncipherment**: folosit pentru a cripta cheile pentru algoritmi simetrici, oferind confidențialitatea datelor,

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

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

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

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

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

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

6.2 Protecția cheii private

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

6.2.1 Standarde pentru modulele criptografice

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

Crearea de semnatura electronica şi criptarea datelor se face conform standardului PKCS#7. Cheile private (ca şi cheile publice) pot fi în una dintre următoarele stări (în conformitate cu standardul ISO/IEC 11770-1):

- **în aşteptare pentru activare** (**pregătită**) – cheia a fost deja generată, dar nu este utilizabilă (data curentă nu este încă aceeaşi cu data începerii perioadei de validitate a certificatului),
- **activă** – cheia poate fi folosită în operațiile criptografice (de exemplu pentru crearea de semnaturii electronice), data curentă este în cadrul perioadei de validitate a certificatului, cheia nu a fost revocată,
- **inactivă** – cheia aflată în această stare poate fi folosită numai pentru verificarea de semnaturii electronice sau pentru operații de decriptare (Abonatului nu-i este permisă folosirea cheii private pentru crearea de semnaturi electronice – validitatea cheii a expirat; în cazul unei chei publice, Abonatului nu îi este permisă criptarea informației); data curentă este în afara perioadei de validitate a certificatului.

6.2.2 Controlul dual al accesului cheii private

Controlul dual a unei chei private se aplică doar cheilor private ale Autorităţilor de Certificare **certSIGN CA Clasa 2**, **certSIGN Qualified CA Clasa 3**, **certSIGN Entreprise CA Clasa 3** şi **certSIGN Non-Repudiation CA Clasa 4** folosite pentru semnarea de certificate şi CRL-uri.

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

Pentru operaţiuni de tipul: iniţierea modulului criptografic hardware, transferul cheilor private ale Autorităţilor de Certificare, se implementează scheme prag de acces (de tip k din n) prin distribuire **de secrete partajate**. Numărul acceptat de secrete partajate şi numărul necesar de secrete care permit restaurarea cheii private sunt expuse în Tabelul 6.2.2.

Autoritatea de emitere certificate	Numărul de secrete partajate	Numărul total de secrete distribuite
certSIGN ROOT CA	2	3
certSIGN CA Class 2	2	3
certSIGN Qualified CA Class 3	2	3
certSIGN Enterprise CA Class 3	2	3
certSIGN Non-Repudiation CA Class 4	2	3

Tabelul 6.2.2. Distribuirea secretelor partajate pentru iniţierea şi transferul cheilor private

Pentru asigurarea serviciului de recuperare a cheilor private ale Abonaţilor se utilizează de asemenea scheme prag de acces. Numărul acceptat de secrete partajate şi numărul necesar de secrete care permit restaurarea cheii private sunt expuse în Tabelul 6.2.3.

Autoritatea de emitere certificate	Numărul de secrete partajate	Numărul total de secrete distribuite
certSIGN CA Class 2	2	3
certSIGN Enterprise CA Class 3	2	3

Tabelul 6.2.3. Distribuirea secretelor partajate pentru recuperarea cheilor de criptare ale utilizatorilor

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

6.2.2.1 Acceptarea păstrării secretului de către deținători

Fiecare deținător de secret partajat, înainte de a primi partea sa de secret, trebuie să asiste personal la împărțirea secretului, să verifice corectitudinea secretului creat şi distribuirea sa. Fiecare parte a secretului partajat trebuie transferată deținătorului pe un card criptografic protejat de un cod PIN, ales de deținător şi ştiut numai de el. Primirea secretului partajat şi crearea sa sunt confirmate printr-o semnatura de mână pe un formular, a cărui copie este păstrată în arhivele Autorității de Certificare şi de către deținătorul de secret.

6.2.2.2 Protecția secretului partajat

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

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

6.2.2.3 Disponibilitatea şi ştergerea (transferul) secretului partajat

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

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

6.2.2.4 Responsabilitățile deținătorului de secret partajat

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

6.2.3 Custodia cheii private

Cheile private de semnare ale Abonatului sau cheile private ale Autorităților de Certificare nu fac obiectul predării în custodie.

6.2.4 Backup-ul cheilor private

Autoritățile de Certificare care operează în cadrul certSIGN creează o copie de siguranță a cheii lor private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgență (de exemplu, după dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secrete partajate.

certSIGN nu păstrează copii ale cheilor private ale operatorilor Autorității de Certificare. Copiile cheilor private ale Abonaților sunt create numai la cererea Abonatului şi în conformitate cu metodele prezentate în 6.2.3.

"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."

6.2.5 Arhivarea cheii private

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

6.2.6 Introducerea cheii private în modulul criptografic

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

- când cheile sunt generate în afara modulului criptografic; această situație apare, de exemplu, în cazul generării cheii de către o Autoritate de Certificare la cererea Abonatului, la introducerea lor într-un dispozitiv criptografic, înainte de trimiterea suportului de stocare către Abonat. O operație similară de introducere a cheii într-un modul criptografic poate fi îndeplinită de un Abonat când cheile sunt livrate sub formă criptată şi necesită stocare locală pe un dispozitiv criptografic,
- în cazul creării copiilor de siguranță ale cheilor private stocate într-un modul criptografic, poate fi necesară, ocazional, (ex. în cazul compromiterii sau defectării modulului) introducerea unei perechi de chei într-un modul de securitate diferit,
- când este necesară transferarea unei chei private din modulul operațional folosit pentru operații standard ale entității, pe un alt modul; situația poate apărea în cazul defectării modulului sau în cazul necesității distrugerii acestuia.

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

Introducerea unei chei private într-un modul hardware de securitate al Autorităților de Certificare **certSIGN ROOT CA** sau **certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4** necesită restaurarea cheii de pe carduri în prezența unui număr corespunzător de

deținători de secret partajat care protejează modulul ce conține cheile private (vezi Capitolul 6.2.2). Deoarece fiecare Autoritate de Certificare poate deține o copie criptată a cheii sale private (vezi Capitolul 6.2.4), cheile pot fi de asemenea transferate între module.

6.2.7 Metoda de activare a cheii private

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

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

Toate cheile private ale **certSIGN ROOT CA** sau **certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4**, introduse în modul după generare, importate sub formă criptată dintr-un alt modul sau restaurate dintr-un secret partajat, rămân în stare activă până la ştergerea lor fizică de pe modul sau până la scoaterea lor din serviciile certSIGN. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea este realizată pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

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

Activarea cheii private a unui Abonat se face în mod similar cu procedura de activare a cheii private a operatorilor Autorității de Certificare, indiferent dacă sunt stocate pe un card criptografic sau sub formă criptată, ca fişier pe o dischetă sau orice alt mediu de stocare. În cazul

Abonaților persoane juridice (organizații, instituții etc.) activarea trebuie să se facă de către o persoană autorizată a Abonatului.

6.2.8 Metoda de dezactivare a cheii private

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

În cazul unui Abonat sau al unui operator al Autorității de Înregistrare, dezactivarea cheii private de semnatura se face imediat după încheierea sesiunii (la ieşire din aplicație). Dacă în timpul executării operației criptografice, cheia privată a fost stocată în memoria aplicației, aplicația trebuie să prevină refacerea neautorizată a cheii private. Dacă o cheie privată este deținută de un Abonat persoană juridică, cheia poate fi dezactivată numai de reprezentantul autorizat al acestui Abonat.

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

6.2.9 Metoda de distrugere a cheii private

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

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

6.3 Alte aspecte cu privire la managementul perechilor de chei

Din punct de vedere tehnologic, este posibilă folosirea aceleiaşi perechi de chei şi pentru crearea de semnaturi electronice şi pentru criptarea datelor. Totuşi acest Cod de Practici şi Proceduri nu

recomandă acest lucru. În cazul certificatelor emise în cadrul politicii certSIGN Clasa 3 şi 4, această practică este interzisă.

Restul cerințelor din acest capitol se referă la procedurile de arhivare a cheii publice şi la perioada de validitate a cheilor publice şi private ale fiecărui Abonat, inclusiv ale Autorităților de Certificare.

6.3.1 Arhivarea cheilor publice

Scopul arhivării cheilor publice este acela de a crea posibilitatea verificării semnaturii electronice după eliminarea unui certificat din depozit (vezi Capitolul 2.6). Acest lucru este foarte important în cazul serviciilor de ne-repudiere, cum ar fi serviciul de marcă temporala sau serviciul de verificare a stării unui certificat.

Arhivarea cheilor publice presupune arhivarea certificatelor care conțin aceste chei.

Fiecare autoritate care emite certificate arhivează cheile publice ale Abonaților către care au fost emise certificatele. Cheile publice ale Autorității de Certificare sunt arhivate împreună cu cheile private, în modul descris în Capitolul 6.2.5. Certificatele pot fi, de asemenea, arhivate local de către Abonați, în special când acest lucru este cerut de aplicațiile folosite (de exemplu, sistemele de poştă electronica).

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

În cadrul certSIGN, numai cheile folosite pentru verificarea semnaturii electronice fac obiectul arhivării. Orice alt tip de chei publice (ex. chei folosite la criptarea mesajelor) sunt distruse imediat după scoaterea lor din depozit.

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

Cheile publice sunt păstrate în arhivele cu certificate digitale 15 ani după momentul expirării, conform tabelului 4.4.

6.3.2 Perioadele de folosire a cheilor private şi publice

Perioada de folosire a cheilor publice este definită de valoarea câmpului validitate a fiecărui certificat de cheie publică (vezi Capitolul 7.1). Există, de asemenea, şi o perioadă de validitate a cheii private. Perioada maxima de utilizare a cheilor Abonaților nu poate depăşi de 2 ori durata de viata a unui certificat, care este specificata mai jos.

Valorile standard ale perioadei maxime de folosire a certificatelor Autorității de Certificare sunt descrise în Tabelul 6.3.2.1, iar a certificatelor Abonaților sunt descrise în Tabelul 6.3.2.2.

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

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

Deținătorul cheii	Scopul principal al folosirii cheii
	RSA pentru semnarea de certificate şi CRL
certSIGN ROOT CA	25 ani
certSIGN Demo CA Class1	10 ani
certSIGN CA Class 2	10 ani
certSIGN Qualified CA Class 3	10 ani
certSIGN Enterprise CA Class 3	10 ani
certSIGN Non-Repudiation CA Class 4	10 ani

Tabelul 6.3.2.1 Perioada maximă de folosire a certificatelor CA

Deținătorul cheii	Politica de certificare	Main key usage
Operatorul Autorității de Înregistrare	certSIGN Clasa 2	1 an
	certSIGN Clasa 3	1 an
	certSIGN Clasa 4	3 ani
Persoanele fizice şi echipamentele hardware ale acestora	certSIGN Clasa 1	3 luni
	certSIGN Clasa 2	1 an
	certSIGN Clasa 3	1 an
	certSIGN Clasa 4	2 ani
Persoanele juridice şi	certSIGN Clasa 1	3 luni

echipamente hardware ale persoanelor fizice	certSIGN Clasa 2	1 an
	certSIGN Clasa 3	1 an
	certSIGN Clasa 4	3 ani

Tabelul 6.3.2.2. Perioadele maxime de folosire a certificatelor Abonaților

6.3.3 Managementul cheilor abonatilor

certSIGN nu furnizeaza niciun fel de serviciu de management al cheilor abonatilor.

6.4 Datele de activare

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

6.4.1 Generarea şi instalarea datelor de activare

Datele de activare sunt folosite în două situații principale:

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

Operatorii Autorității de Înregistrare şi ai Autorităților de Certificare, precum şi alte persoane care îndeplinesc rolurile descrise în Capitolul 5.2, trebuie să folosească parole rezistente la atacuri prin încercări repetate (forța brută). Se recomandă ca şi Abonații să folosească astfel de parole.

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

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

Secretele partajate folosite pentru protejarea cheii private a Autorității de Certificare sunt generate în concordanță cu cerințele prezentate în Capitolul 6.2 şi păstrate pe carduri criptografice. Cardurile sunt protejate printr-un cod PIN, creat în concordanță cu cerințele FIPS-

112. Secretele partajate devin date de activare după activarea acestora, de exemplu, prin introducerea corectă a codului PIN care protejează cardul.

6.4.2 Protecția datelor de activare

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

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

6.4.3 Alte aspecte cu privire la datele de activare

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

6.5 Controalele de securitate a calculatoarelor

Sarcinile operatorilor Autorității de Înregistrare şi ai Autorității de Certificare care lucrează în cadrul certSIGN sunt realizate prin intermediul unor dispozitive hardware şi aplicații software de încredere.

6.5.1 Cerințele tehnice specifice securității calculatoarelor

Cerințele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor şi aplicațiilor, folosite în cadrul certSIGN. Măsurile de securitate care protejează

sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicațiilor precum şi din punct de vedere fizic.

Calculatoarele aparținând Autorităților de Certificare şi componentelor asociate acestora (de exemplu Autoritatea de Înregistrare) dispun de următoarele mijloace de securitate:

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

6.5.2 Evaluarea securității calculatoarelor

Sistemele de calcul certSIGN respectă cerințele descrise în standardele ETSI: ETSI TS 101456 (Cerințele de Politică pentru Autoritățile de Certificare care emit certificate calificate) şi CEN CWA 14167 (Cerințele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnatura Electronica).

6.6 Controale tehnice specifice ciclului de viata

6.6.1 Controale specifice dezvoltării sistemului

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

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

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

6.6.2 Controale pentru managementul securității

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

Configurația curentă a sistemelor certSIGN, precum şi orice modificare şi actualizare a acestora, este înregistrată şi controlată.

Controalele aplicate sistemelor certSIGN permit verificarea continuă a integrității aplicațiilor, versiunii şi autentificarea şi verificarea originii dispozitivelor hardware.

6.7 Controale de securitatea a rețelei

Serverele şi stațiile de lucru de încredere aparținând certSIGN sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subretele, cu acces controlat. Accesul dinspre Internet către orice segment, este protejat prin intermediul unui firewall inteligent.

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

Mijloacele de asigurare a securității rețelei acceptă doar mesajele transmise prin protocoalele http, https, NTP, POP3 şi SMTP. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem şi permit supravegherea folosirii corecte a serviciilor furnizate de certSIGN.

6.8 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerințele impuse pentru dezvoltarea, producția şi livrarea modulelor. certSIGN nu defineşte cerințe specifice în acest domeniu. Totuşi, certSIGN acceptă şi utilizează numai module criptografice care corespund cerințelor din Capitolul 6.2.

7 Profilul certificatelor, CRL şi OCSP

Profilul certificatelor şi al Listei de certificate Revocate (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerințele RFC 2560. Informațiile de mai jos descriu semnificația câmpurilor din certificat, CRL şi OCSP, standardul aplicat şi extensiile folosite de certSIGN.

7.1 Profilul certificatelor

Conform standardului X.509 v.3, un certificat este alcătuit din următoarea secvență de câmpuri: corpul certificatului (**tbscertificate**), informații despre algoritmul folosit pentru semnarea certificatului (**signatureAlgorithm**), şi semnatura electronica propriu-zisă a Autorității de Certificare (**signatureValue**).

7.1.1 Conținutul certificatului

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

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

7.1.1.1 Câmpurile de baza

certSIGN acceptă următoarele câmpuri de bază:

- **Version**: a treia versiune (X.509 v.3) a formatului de certificat,
- **SerialNumber**: numărul serial al certificatului, unic în cadrul domeniului Autorității de Certificare,
- **signatureAlgorithm**: identificatorul algoritmului de semnatura folosit de Autoritatea de Certificare emitentă,
- **Issuer**: numele distinctiv (ND) al Autorității de Certificare ,

- **Validity**: perioada de validitate, descrisă prin intermediul unei date de începere (**notBefore**) şi a unei date de expirare (**notAfter**) a certificatului,
- **Subject**: numele distinctiv (ND) al Abonatului care este subiectul certificatului,
- **SubjectPublicKeyInfo**: valoarea cheii publice împreună cu identificatorul algoritmului criptografic folosit.

În certificatele emise de certSIGN, valorile câmpurilor de mai sus sunt stabilite în concordanţă cu regulile descrise în Tabelul 7.1.

Numele câmpului	Valoarea sau restricţiile valorii	
Version	Versiunea 3	
Serial Number	Valoare unică pentru toate certificatele emise de Autorităţile de Certificare din cadrul certSIGN	
SIGNature Algorithm	md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) sau sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (Distinguished Name)	Numele (CN) =	certSIGN {CA Class {1,2,3,4}}
	Organizaţia (O) =	certSIGN
	Ţara (C) =	RO
Not before (data de începere a perioadei de validitate)	În baza sistemului universal de referinţă temporala (Universal Time Coordinated). certSIGN poseda un ceas controlat de Atomic Frequency Standard.	
Not after (data de expirare a perioadei de validitate)	În baza sistemului universal de referinţă temporala (Universal Time Coordinated). certSIGN poseda un ceas controlat de Atomic Frequency Standard.	
Subject (Distinguished Name)	Numele distinctiv respectă cerinţele standardului X.501. Valorile unora dintre atributele acestor câmpuri sunt opţionale şi semnificaţia lor este descrisa mai jos.	
Subject Public Key Info	Criptat în conformitate cu RFC 3280, poate conţine informaţii despre cheile publice ale RSA, DSA sau ECDSA (identificatorul cheii, mărimea cheii în biţi şi valoarea cheii publice); mărimea cheii RSA este prezentată în Capitolul 6.1.5.	
Signature	Semnatura certificatului, generată şi criptată în conformitate cu cerinţele descrise în RFC 3280.	

Tabel 7.1. Profilul câmpurilor de baza ale certificatelor

Profilele tuturor certificatelor (câmpurile din Subject):

Certificat simplu personal nominal semnare/criptare/semnare cod

Obligatoriu: Nume, Prenume, Tara, email

Opţional: n/a

Nume în clar:

Subject: C=Țara, CN=Prenume Inițiala Nume

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificat simplu personal anonim semnare/criptare

Obligatoriu: Pseudonim, Tara, email

Opțional: n/a

Pseudonim:

Subject: C=Țara, CN=Pseudonim

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificat simplu profesional nominal semnare/criptare

Obligatoriu: Nume, Prenume, Tara, Organizație, Localitate, email

Opțional: Departament, Funcție

Nume în clar :

Subject : C=Țara, O=Organizație, OU=Departament*, CN = Prenume Inițiala Nume, T* = Funcție, L = Localitatea

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificat simplu persoane juridice/profesional pentru semnare cod

Persoane juridice :

Subject : C=Țara, O=Organizație, OU=Departament*, CN = Denumirea persoanei juridice, L = Localitatea

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificat calificat personal nominal

Obligatoriu: Nume, Prenume, Tara, Localitate, email

Opțional : Telefon, Județ/Sector, Strada, Nr., Bloc, Apartament, Cod Poştal

Nume în clar :

Subject : C=Țara, CN=Prenume Inițiala Nume, Phone*=Telefon, Serial Number = Cod Personal de Identificare, L = Localitate, STREET*=Adresa (Strada, Nr, Bloc, Scara, Apartament, CodPostal), S*=Judet/Sector, 2.5.4.41(Name)=Prenume Inițiala Nume, G=Prenume, SN=Nume

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificat calificat personal anonim

Obligatoriu: Pseudonim, Tara, Localitate, email

Opțional: n/a

Pseudonim :

Subject : C=Țara, P=Pseudonim, Serial Number = Cod Personal de Identificare, L = Localitate, S=Judet/Sector

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificat calificat profesional nominal

Obligatoriu: Nume, Prenume, Organizație, Tara, Localitate, email

Opțional: Departament, Funcție, Telefon, Judet/Sector, Strada, Nr., Bloc, Apartament, Cod Poştal

Nume în clar :

Subject : C=Țara, O=Organizația, OU*=Departament, CN=Prenume Inițiala Nume, T*=Funcție, Phone*=Telefon, Serial Number=Cod Personal de Identificare, L=Localitate, STREET*=Adresa (Strada, Nr, Bloc, Scara, Apartament, CodPostal), S*=Judet/Sector, 2.5.4.41(Name)=Prenume Inițiala Nume, G=Prenume, SN=Nume

Certificate calificate persoane juridice

Obligatoriu: Numele persoanei juridice, Tara, Localitate, email

Opțional: Telefon, Judet/Sector, Strada, Nr., Bloc, Apartament, Cod Poştal

Certificate calificate persoane juridice:

Nume în clar:

Subject :C=Țara, O=Organizația, CN=Numele persoanei juridice, Phone*=Telefon, Serial Number=Cod Unic de Identificare, L=Localitate, STREET*=Adresa (Strada, Nr, Bloc, Scara, Apartament, CodPostal), S*=Județ/Sector

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Certificate web si VPN

Subject: Este dat de campul subject din cererea de certificat in format PKCS10 a serverului web, sau a dispozitivului VPN, cu conditia ca clientul sa demonstreze ca informatia respectiva din continutul campului subject reprezinta date de identificare pe care acesta este autorizat sa le foloseasca.

Subject Alternative Name: DNS=optional numele serverului, IP Address=optional adresa IP a serverului

7.1.1.2 Extensii standard

Rolul fiecărei extensii este definit de valoarea standard a identificatorului de obiect folosit (**OBJECT IDENTIFIER**). Extensia, funcție de opțiunea autorității emitente, poate fi **critică** sau **ne-critică**. Dacă o extensie este definită ca fiind **critică**, aplicația care foloseşte certificatul trebuie să respingă orice certificat care conține o extensie critică nerecunoscută. Pe de altă parte, extensiile definite ca fiind **ne-critice** pot fi omise.

certSIGN acceptă următoarele câmpuri de extensii standard:

- **AuthorityKeyIdentifier**: identificatorul certificatului de cheie publică al Autorității de Certificare, asociat cheii private folosită pentru semnarea certificatelor – **această extensie nu este critică**,

- **SubjectKeyIdentifier** – identificatorul cheii subiectului - **această extensie nu este critică**,
- **KeyUsage**: scopul în care poate fi folosită cheia - **această extensie este critică**. Extensia descrie pentru ce poate fi utilizată o cheie, de exemplu, pentru criptarea de date, pentru schimbul de date, pentru semnarea electronica etc.:

  digitalsignature (0) – cheie pentru crearea de semnaturi electronice

  nonRepudiation (1) – cheie asociată cu serviciile de ne-repudiere

  keyEncipherment (2) – cheie pentru schimbul de chei,

  dataEncipherment (3) – cheie pentru criptarea datelor

  keyAgreement (4) – cheie pentru negocierea de chei

  keycertsign (5) – cheie pentru semnarea de certificate

  CRLsign(6) – cheie pentru semnarea de CRL-uri

  encipherOnly (7) – cheie numai pentru criptare

  decipherOnly (8) – cheie numai pentru decriptare

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

  serverAuth – autentificarea severelor Web TLS; **keyUsage** are setaţi biţii pentru: digitalSIGNature, keyEncipherment sau keyAgreement;

  clientAuth – autentificarea clienţilor Web TLS; **keyUsage** are setaţi biţii pentru: digitalsignature şi /sau keyAgreement;

  codesigning – semnarea codurilor executabile; **keyUsage** are setat bitul pentru digitalsignature;

emailProtection – protecția e-mail-ului; **keyUsage** are setați biții pentru: digitalsignature, non-Repudiation şi/sau (keyEncipherment sau keyAgreement),

ipsecEndSystem – protocolul de protecție IPSEC,

ipsecTunnel – protocolul IPSEC Tunnelling,

ipsecUser – protocolul de protecție IP al aplicațiilor utilizatorului,

timeStamping – legarea rezumatului (digest) cu timpul furnizat de sursa de încredere**; keyUsage** are setați biții pentru: digitalSIGNature, nonRepudiation.

OCSPsigning – asignează dreptul de a emite confirmări privind starea certificatului în numele lui CA; keyUsage are setați biții pentru: digitalsignature, nonRepudiation.

dvcs – emiterea unei confirmări de către un notar autorizat, pe baza protocolului DVCS; keyUsage are setați biții pentru: digitalSignature, nonRepudiation, keycertSIGN, cRLSIGN.

EncryptedFileSystem – permite folosirea certificatului pentru criptarea sistemului de fişiere (EFS); este cerut obligatoriu de anumite aplicații de acest gen (ex. EFS);

SmartCardLogon – permite utilizarea certificatului pentru operația de „smart-card logon" - autentificare în sistemul de operare, bazată pe certificat digital;

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

Numele Politicii de certificare	Identificatorul Politicii
certSIGN Clasa 1	**{certSIGN}[1] .{id-policy}[2]. {id-cp}[3].{id-Class-1}[4]** =1.3.6.1.4.1.25017.1.1.1

[1] {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (20715); [2] {id-policy}=1; [3] {id-cp}=1;[4] {Class-1}=1

certSIGN Clasa 2	**{certSIGN} id-policy(1) id-cp(1)id-Class-2(2)=** 1.3.6.1.4.1.25017.1.1.2
certSIGN Clasa 3	**{certSIGN} id-policy(1) id-cp(1)id-Class-3(3) =**1.3.6.1.4.1.25017.1.1.3
certSIGN Clasa 4	**{certSIGN} id-policy(1) id-cp(1)id-Class-3(3) =**1.3.6.1.4.1.25017.1.1.4

Tabelul 7.2. Identificatorii politicilor şi numele acestora

certificate emise de către Autoritățile de Certificare includ şi calificatori recomandați de RFC 3280 :

- **PolicyMapping**: map-area politicii – **acest câmp nu este critic**; acest câmp conține una sau mai multe perechi de OID, definind echivalența politicii emitentului certificatului cu politica subiectului certificatului,
- **SubjectAlternativeName:** numele alternativ al subiectului – acest câmp nu este critic;
- **BasicConstraints**: constrângeri de bază – indică tipul certificatului (certificat de CA sau entitate finală), precum şi lungimea maxim admisă pentru lanțul de certificate - **acest câmp este critic** ;
- **CRL DistributionPoints**: punctul de distribuire a Listei certificatelor Revocate – **acest câmp nu este critic**; extensia defineşte adresa din rețea la care se află CRL-ul curent al Autorității emitente a certificatului în cauză
- **AuthorityInfoAccessSyntax**: accesul la informațiile despre Autoritatea de Certificare – **acest câmp nu este critic**; câmpul indică metoda de informare şi furnizare a serviciilor de către emitentul certificatului
- **OCSPNoCheck**: dacă este prezentă în cadrul unui certificat al unui responder OCSP, clienții care primesc răspunsuri OCSP semnate cu o cheie privată asociată certificatului pot avea încredere cu privire la starea acestui certificat pe perioada sa de valabilitate; această extensie **este ne-critică** şi este definită de standardul RFC 2560
- **NetscapeCertType**: această extensie limitează utilizarea certificatului numai la anumite aplicații specificate de valoarea extensiei. Dacă nu este prezentă, certificatul poate fi folosit pentru orice aplicație cu excepția aplicațiilor de ObjectSigning. Extensia **este ne-critică**, iar valoarea să poate fi o combinație din următoarele:

  SSLClient (bit 0) – certificatul poate fi folosit pentru autentificarea unui client SSL

SSLServer (bit 1) – certificatul poate fi folosit pentru autentificarea unui server SSL

S/MIME (bit 2) – certificatul poate fi folosit de clienți de mail securizat S/MIME

ObjectSigning (bit 3) - certificatul poate fi folosit pentru semnarea obiectelor cum ar fi 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

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

7.1.2 Extensiile certificatelor

certificatele emise de către certSIGN pot conține diferite combinații ale extensiilor definite în 7.1.1.2.

7.1.2.1 Certificatele Autorităților de Certificare

Certificatele Autorităților de certificare pot conține extensiile din Tabelul 7.3. şi 7.4

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5), cRLSign (bit 6)	critică

Tabelul 7.3. Extensiile certificatului certSIGN Root CA

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5), cRLSign (bit 6)	critică
CRL Distribution Points	http://crl.certsign.ro/root.crl ldap://ldap.certsign.ro/C=RO,O=certSIGN,OU=certSIGN Root CA	ne-critică

	?certificateRevocationList;binary	
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1.{2,3,4} CPS: http://www.certsign.ro/repository	ne-critică

Tabelul 7.4. Extensiile certificatelor pentru Autoritățile Subordonate (Clasele 2-4)

7.1.2.2 Certificatele pentru autentificarea serverelor

Certificatele pentru autentificarea serverelor Web pot conține extensiile din Tabelul 7.5.

Extensia	Valoarea sau restricția valorii	Starea extensiei
Basic Constraints	Subject type = End Entity, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), keyEncipherment (bit 2)	critică
ExtendedKeyUsage	serverAuth, clientAuth	ne-critică
Netscape Cert Type	SSLServer (bit 1)	ne-critică
Subject Alternative Name	DNS.1: Full DNS service name	ne-critică
CRL Distribution Points	http://crl.certsign.ro/enterprise.crl ldap://ldap.certSIGN.ro/CN=certSIGN Enterprise CA Class 3,OU=certSIGN Enterprise CA Class 3,O=certSIGN,C=RO?certificateRevocationList;binary	ne-critică
Authority Info Access	OCSP: http://ocsp.certsign.ro	ne-critică
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1.3 CPS: http://www.certsign.ro/repository	ne-critică

Tabelul 7.5. Extensiile certificatelor pentru autentificarea serverelor

7.1.2.3 Certificatele pentru semnarea codului

Certificatele pentru semnarea codului pot conține extensiile specificate în Tabelul 7.6.

Extensia	Valoarea sau restricția valorii	Starea extensiei
Basic Constraints	Subject type = End Entity, Path length constraint=none	critică
Key Usage	digital signature (bit 0), non-repudiation (bit 1)	critică
Extended Key Usage	codeSigning	ne-critică
Netscape Cert Type	ObjectSigning (bit 3)	ne-critica
Subject Alternative Name	RFC822 Name (ex. customer@somewhere-in-world.com)	ne-critică
CRL Distribution Points	http://crl.certsign.ro/enterprise.crl ldap://ldap.certsign.ro/CN=certSIGN Enterprise CA Class 3,OU=certSIGN Enterprise CA Class 3,O=certSIGN,C=RO?certificateRevocationList;binary.	ne-critică
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	ne-critică
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1..3 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.6. Extensiile certificatelor pentru semnare de cod

7.1.2.4 Certificatele pentru entitățile persoane fizice sau juridice

Certificatele emise Abonaților persoane fizice şi juridice (inclusiv certificatele pentru criptarea sistemului de fişiere – certificate EFS, certificatele de smartcard logon, certificate pentru schimbul electronic de date – certificate EDI, certificate calificate în concordanță cu standardul RFC 3039) pot conține extensiile specificate în Tabelul 7.7

Extensia	Valoarea sau restricția valorii	Starea extensiei
Basic Constraints	Subject type = End Entity, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyEncipherment (bit 2) dataEncipherment (bit 3), keyAgreement (bit 4)	critică
Extended Key Usage	clientAuth, emailProtection, EncryptedFileSystem, SmartCardLogon	ne-critică
NetscapeCertType	SSLClient (bit 0), S/MIME (bit 2)	ne-critică
Subject Alternative Name	RFC822 Name: customer@somewhere-in-world.com, *UPN	ne-critică
CRL Distribution Points	dependant on issuing CA-see the other profiles ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class{2,3,4}?certificateRevocationList;binary	ne-critică
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	ne-critică
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.{2,3,4} CPS: http://www.certSIGN.ro/repository itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1) – în cazul certificatelor calificate	ne-critică

Tabelul 7.7. Extensiile certificatelor emise entităților persoane fizice sau juridice

7.1.2.5 certificatele pentru Rețele Virtuale Private (certificatele VPN)

certificatele pentru crearea de Rețele Virtuale Private (VPN) pot conține extensiile specificate în Tabelul 7.8.

Extensia	Valoarea sau restricția valorii	Starea extensiei
Basic Constraints	Subject type = End Entity, Path length constraint=none	Critică
Key Usage	digitalSignature (bit 0), keyEncipherment (bit 2)	Critică
Extended Key Usage	IpsecUser, IpsecTunnel, IpsecEndSystem	ne-critică
Subject Alternative Name	DNS: full VPN router domain name (FQDN) IP: VPN router IP address	ne-critică
CRL Distribution Points	http://crl.certsign.ro/enterprise.crl ldap://ldap.certsign.ro/CN=certSIGN Enterprise CA Class 3,OU=certSIGN Enterprise CA Class 3,O=certSIGN,C=RO?certificateRevocationList;binary.	ne-critică

Authority Info Access	OCSP: http://ocsp.certSIGN.ro	ne-critică
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.3 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.8. Extensiile certificatelor VPN

7.1.2.6 Cross-certificarea şi certificatele de ne-repudiere

certificatele pentru cross-certificare şi certificatele de ne-repudiere pot conţine extensiile specificate în Tabelele 7.9, 7.10 şi 7.11.

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint={none,1,2,...}	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5) cRLSign (bit 6)	critică
CRL Distribution Points	URI: http://crl.certSIGN.ro/class4.crl ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class 4?certificateRevocationList;binary	ne-critică
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	ne-critică
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.9. Extensiile certificatelor de cross-certificare

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=End Entity, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	critică
Extended Key Usage	OCSPSigning	ne-critică
OCSPNoCheck	-	ne-critica
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.10. Extensiile certificatelor de Autoritate de OCSP

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=EndEntity, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	critică
Extended Key Usage	timeStamping	ne-critică
CRL Distribution Points	URI: http://crl.certSIGN.ro/class4.crl ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class 4?certificateRevocationList;binary	ne-critică

Authority Info Access	OCSP: http://ocsp.certSIGN.ro	ne-critică
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.11. Extensiile certificatelor de Autoritate TimeStamp

Pe lângă extensiile prezentate mai sus, în certificate se pot introduce la cererea clientului şi alte extensii particulare, în condiţii stabilite la momentul contractului.

7.1.3 Identificatorul algoritmului de semnare

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

7.1.4 Câmpul ce conţine semnatura electronica

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

7.2 Profilul CRL

Lista de certificate Revocate (CRL) constă din trei câmpuri. Primul câmp (**tbscertList**) conţine informaţii despre certificatele revocate, al doilea şi al treilea câmp – **signatureAlgorithm** şi **signatureValue** conţin informaţii despre identificatorul algoritmului folosit pentru semnarea listei şi semnatura electronica a Autorităţii de Certificare.

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

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

- **Version**: versiunea formatului de CRL,

- **signature**: identificatorul algoritmului folosit de Autoritatea de Certificare pentru a semna CRL-ul; autoritățile certSIGN semnează CRL-urile folosind algoritmul **sha1WithRSAEncription**,
- **Issuer**: numele Autorității de Certificare care a emis CRL-ul; fiecare autoritate a certSIGN emite propria sa Listă de certificate Revocate; acest lucru se aplică următoarelor autorități: **certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Entreprise CA Class 3** şi **certSIGN Non-Repudiation CA Class 4,**
- **ThisUpdate**: data publicării CRL-ului,
- **NextUpdate**: date la care se va publica următorul CRL; dacă câmpul este prezent, valoarea sa descrie data maximă până la care se va face actualizarea CRL-ului,
- **Revokedcertificates**: lista certificatelor revocate (câmpul este gol în cazul în care nu a fost revocat nici un certificat); informația constă din trei sub-câmpuri:

  usercertificates – numărul serial al certificatului revocat;

  revocationDate – data revocării certificatului;

  crlEntryExtensions – conține informații suplimentarea despre certificatele revocate - opțional.

- **crlExtensions**: informații suplimentare despre Lista de certificate Revocate (câmp opțional). Dintre extensiile posibile, cele mai importante sunt următoarele: **AuthorityKeyIdentifier** (vezi şi Capitolul 7.1.1.2) care permite identificarea cheii publice corespunzătoare cheii private folosită pentru semnarea listei şi **cRLNumber**, care conține un număr serial incrementat monoton al listei emisă de Autoritatea de Certificare (prin intermediul acestei extensii, Abonatul are posibilitatea de a determine dacă a fost publicat un nou CRL).

7.2.1 Extensiile acceptate în intrările din CRL

Rolul şi semnificația extensiilor este aceleaşi ca în cazul extensiilor de certificat (vezi Capitolul 7.1.1.2). Extensiile dintr-o intrare CRL (**crlEntryExtensions**) acceptate de certSIGN- conțin următoarele câmpuri:

- **ReasonCode**: codul motivului revocării certificatului. **Acest câmp nu este critic** şi permite determinarea motivului revocării unui certificat. Sunt permise următoarele motive de revocare:

  unspecified – nespecificat;

  keyCompromise – compromiterea cheii;

  cACompromise – compromiterea cheii Autorității de Certificare;

  affiliationChanged – modificarea datelor Abonatului;

  superseded – înnoirea certificatului;

  cessationOfOperation – sistarea folosirii certificatului;

  removeFromCRL – eliminarea certificatului din CRL.

7.2.2 Certificatul revocat şi CRL

Listele de certificate revocate se păstrează pentru o perioada de minim 15, conform tabelului 4.4. Certificatele revocate sunt scoase din lista de certificate revocate după expirare.

7.3 Profilul răspunsului de confirmare OCSP

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

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

Certificatul serverului OCSP trebuie să conțină extensia extKeyUsage, descrisă în RFC 3280. Această extensie trebuie declarată ca fiind ne-critică şi semnifică faptul că o Autoritate de Certificare care emite certificatul pentru serverului OCSP confirmă prin semnatura sa delegarea autorizării de a emite confirmări ale stării certificatelor (aparținând Abonaților acestei autorități).

De asemenea, certificatul serverului OCSP conține extensia OCSPNoCheck, descrisă de RFC 2560. Această extensie trebuie declarată ca fiind ne-critică şi semnifică faptul că un client de OCSP care primeşte un răspuns semnat cu cheia privată asociată acestui certificat va putea avea

încredere în starea certificatului serverului OCSP, nefiind necesară verificarea stării de revocare a acestuia.

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

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

7.3.1 Numărul versiunii

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

7.3.2 Informațiile despre starea certificatului

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

- GOOD – indică faptul că certificatul este în stare validă

- REVOKED – indică faptul că certificatul a fost emis şi a fost revocat

- UNKNOWN – indică faptul că nu există suficiente informații pentru determinarea stării certificatului respectiv

7.3.3 Extensiile standard acceptate

În concordanță cu RFC 2560, serverul OCSP al certSIGN acceptă următoarea extensie:

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

8 Managementul Codului de Practici şi Proceduri

Fiecare versiune a Codului de Practici şi Proceduri este în vigoare (starea sa este **valida**) până în momentul publicării şi aprobării noii sale versiuni (vezi Capitolul 8.3). O nouă versiune este dezvoltată de către certSIGN şi publicata pentru comentarii cu mențiunea **spre aprobare** (daca este cazul). După primirea şi includerea comentariilor, Codul de Practici şi Proceduri intra în procedura de aprobare interna. Responsabil de aprobarea formei finale a Codului de Practici si Proceduri este un comitet format din directorul general, directorul general adjunct, managerii departamentelor tehnice si managerul departamentului de dezvoltare a afacerii. Responsabil pentru intretinerea Codului de Practici si Proceduri este managerul departamentului care asigura furnizarea serviciilor de certificare. După terminarea procedurii de aprobare, noua versiune a CPP este transmisa Autorității de Reglementare şi Supraveghere si apoi, in teremen de 10 zile, este publicata şi marcată ca fiind în starea **validă**. Regulile şi cerințele descrise mai jos, cu privire la managementul Codului de Practici şi Proceduri guvernează şi managementul Politicii de certificare.

Abonații trebuie să respecte numai Politica de certificare şi Codul de Practici şi Proceduri în vigoare în momentul respectiv.

8.1 Procedura de schimbare a CPP

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

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

Modificările introduse pot fi în general împărțite în două categorii: una care nu necesită consultarea Abonaților şi una care cere (de obicei în avans) consultarea Abonaților. Prima categorie include modificari de urgenta sau modificari neesentiale.

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

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

8.2 Procedurile de publicare şi notificare

O copie a Codului de Practici şi Proceduri este disponibilă în formă electronica pe site-ul de Web http://www.certSIGN.ro/repository sau prin e-mail la adresa office@certSIGN.ro. Trei versiuni ale Codului de Practici şi Proceduri sunt întotdeauna disponibile în Depozit şi prin e-mail: versiunea în vigoare, versiunea anterioară şi versiunea în curs de aprobare (daca este cazul).

8.3 Procedurile de aprobare a CPP

Dacă în timp de 30 de zile de la data publicării propunerilor de modificare ale Codului de Practici şi Proceduri, certSIGN nu primeşte remarci semnificative cu privire la aceste schimbări, noua versiune a Codului de Practici şi Proceduri, aflata în starea **spre aprobare,** devine documentul care guvernează politica de certificare şi trebuie respectat de toți Abonații certSIGN iar starea acestei versiuni va fi schimbată în **validă**.

Abonații care nu acceptă noul Cod de Practici şi Proceduri, conținând termenii şi reglementările modificate, sunt obligați să depună, în termen de 15 zile de la data la care noua versiune a Codului de Practici şi Proceduri a fost aprobată, o declarație în acest sens. Acest lucru duce la încetarea contractului de presari servicii de certificare şi la revocarea certificatului emis în baza acestuia.

Anexa 1: Glosar

Abonat – entitate (persoană fizică sau juridică, unitate organizațională fără identitate juridică, dispozitiv hardware deținut de aceste entități sau persoane) care: (1) este subiectul certificatului emis acestei entități, (2) posedă o cheie privată asociată certificatului emis pentru această entitate şi (3) nu emite certificate altor entități.

Acces – abilitatea de a folosi o resursă informaționala din sistem

Actualizarea de certificat – înainte de expirarea unui certificat, CA îl poate actualiza (sau înnoi) confirmând validitatea aceleiaşi perechi de chei pentru următoarea perioadă de validitate (în concordanță cu Politica de certificare).

Audit – executarea unor proceduri independente de verificare şi evaluare cu scopul de a testa măsura în care este suficient şi adecvat managementul implementat pentru controlul sistemului, de a verifica dacă operațiile sistemului sunt îndeplinite în conformitate cu Politica de certificare acceptată şi cu celelalte reglementări care decurg din ea, de a descoperi posibilele breşe de securitate şi de a recomanda modificarea corespunzătoare a măsurilor de control, a politicii de certificare şi a procedurilor aferente.

A autentifica – a confirma identitatea declarată a unei entități

Autentificare – controlul de securitate cu scopul de a oferi siguranță şi încredere datelor transferate, mesajelor sau emitenților lor; controalele de verificare a autenticității unei persoane, înainte de a-i livra un tip de informații secreta

Calea de certificare – calea ordonată a certificatelor, pornind de la un certificat considerat punct de încredere (ales de verificator) până la certificatul de verificat. O cale de certificare îndeplineşte următoarele condiții:

- pentru toate certificatele cert(x) incluse în calea de certificare {cert(1), cert(2), ……., cert(n-1)} subiectul certificatului cert(x) este emitentul certificatului cert(x+1),
- certificatul cert(1) este emis de o Autoritate de Certificare (punct de încredere) considerată de încredere de către verificator,
- cert(n) este certificatul de verificat.

Fiecare cale de certificare poate fi legată de una sau mai multe politici de certificare sau o astfel de politică poate fi inexistentă. Politicile atribuite unei căi de certificare sunt intersecția politicilor a căror identificatori sunt incluşi în fiecare certificat, încorporate în calea de certificare şi definite în extensia certificatePolicies.

certificatul de cheie publică – o structura de date care conține cel puțin numele sau identificatorul unei Autorități de Certificare , identificatorul unui Abonat, cheia sa publică, perioada de validitate, numărul serial şi cel asignat de către Autoritatea de Certificare. Un certificat poate fi în una din trei stări fundamentale: în aşteptarea activării, activ şi inactiv.

certificat Valid – un certificat de cheie publică este valid numai atunci când (1) a fost emis de o Autoritate de Certificare (2) a fost acceptat de Abonat (subiectul certificatului) şi (3) nu a fost revocat.

certificat revocat – certificat de cheie publică plasat pe Lista certificatelor Revocate.

Cheie secretă - cheie folosită în tehnicile criptografice simetrice, cunoscuta doar de un grup de Abonaţi autorizaţi.

Cheie privată – una dintre cheile asimetrice aparţinând unui Abonat şi folosita numai de acel abonat. În cazul sistemelor cu chei asimetrice, o cheie privată descrie transformarea de semnare. În cazul sistemului asimetric de criptare, o cheie privată descrie transformarea de decriptare. Cheia privata este (1) cheia al cărei scop este decriptarea sau crearea de semnatura pentru uzul exclusiv al proprietarului; (2) acea cheie din pereche de chei care este cunoscută numai proprietarului.

Cheie publică – una dintre cheile perechii asimetrice ale unui Abonat, care este disponibilă publicului. În cazul sistemelor de criptare asimetrică, cheia publică defineşte transformarea de verificare a semnaturii. În cazul criptării asimetrice, cheia publică defineşte transformarea de criptare a mesajelor.

Control al accesului – procesul de acordare a accesului la resursele informaţionale de sistem numai utilizatorilor autorizaţi, aplicaţiilor, proceselor şi altor sisteme.

Cross-certificat – certificat de cheie publică emis unei Autorităţi de Certificare, conţinând nume diferite pentru emitent şi subiect; cheia publică a acestui certificat poate fi folosită numai pentru verificarea semnaturii electronice. Se indică clar că certificatul aparţine unei Autorităţi de Certificare .

Cross-certificare – procedură de emitere a unui certificat, de către o Autoritate de Certificare, pentru o altă Autoritate de Certificare, care nu este direct sau indirect afiliată autorităţii emitente. De obicei, un cross-certificat este emis pentru a simplifica construirea şi verificarea căilor de certificare care conţin certificate emise de diferite CA. Emiterea unei cross-certificat poate fi executată pe baza unui acord reciproc intre două Autorităţi de Certificare, care îşi emit cross-certificate una celeilalte.

Datele auditului – înregistrările cronologice ale activităţii sistemului care să permită reconstituirea şi analiza secvenţelor de evenimente şi modificările sistemului asociate evenimentelor înregistrate.

Deţinător de secret partajat – deţinător autorizat al unui card electronic folosit pentru păstrarea secretului partajat.

Dovada de posesie a cheii private – informaţiile trimise de un Abonat astfel încât să permită primitorului să verifice validitatea legăturii dintre expeditor şi cheia sa privată, accesibilă numai expeditorului; metoda de dovedire a posesiei cheii private depinde de tipul de chei folosite, de ex. în cazul cheilor de semnare este suficientă prezentarea unui text semnat (verificarea cu succes a semnaturii este dovada posesiei cheii private), în timp ce în cazul cheilor de criptare, Abonatul trebuie să poată decripta informaţiile criptate cu cheia publică aflată în posesia sa. certSIGN îndeplineşte verificările asocierii dintre perechile de chei folosite pentru semnare şi criptare numai la nivelul Autorităţii de Înregistrare şi a Autorităţii de Certificare.

Entitate finala – entitate autorizată, care foloseşte certificatul ca un Abonat sau ca o Entitate Perteneră (nu se aplică Autorităţilor de Certificare)

Entitatea Parteneră – primitorul informaţiilor conţinând un certificat sau o semnatura electronica asociată, verificată cu o cheie publică inclusă în certificat şi care trebuie să decidă dacă acceptă sau respinge semnatura pe baza încrederii în certificat.

Furnizor de servicii de certificare – instituţie de încredere (inclusiv dispozitivele hardware aflate sub controlul sau) care face parte dintre terţii de încredere şi care furnizează servicii capabile să creeze, să semneze şi să emită certificate sau servicii de ne-repudiere.

Identificator de obiect (OID) – identificator alfanumeric / numeric înregistrat în concordanță cu standardul ISO/IEC 9834 şi oferind unicitate unui obiect specificat sau clasei sale.

Infrastructura de cheie publică (PKI) – arhitectura, tehnicile, practicile şi procedurile care contribuie în mod colectiv la implementarea şi funcționarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware şi software, baze de date, resurse de rețea, proceduri de securitate şi obligații legale, legate împreună şi care colaborează pentru a furniza şi implementa atât serviciile de certificare cât şi alte servicii asociate infrastructurii (de ex. furnizarea de marcă temporala).

Jeton (token) – structura de date folosita pentru schimbul dintre entități şi care conține informații transformate prin tehnici criptografice. Jetonul este semnat de operatorul unei Autorități de Înregistrare şi poate fi folosit pentru autentificarea deținătorului său în relația sa cu Autoritatea de Certificare.

Lista de certificate Revocate (CRL) – listă emisă periodic sau imediat, semnată electronic de către o autoritate, permițând identificarea certificatelor care au fost revocate sau suspendate înainte de expirarea perioadei de validitate. CRL conține numele emitentului său, data publicării, data următoarei actualizări, numerele seriale ale certificatelor revocate sau suspendate şi datele şi motivele revocării sau suspendării lor.

Modul criptografic – un dispozitiv care constă în hardware, software, microcod sau o combinație a lor şi care execută operațiile criptografice (inclusiv criptare şi decriptare) în interiorul zonei acestui modul criptografic.

Nume Distinctiv (DN) – un set de atribute care formează un nume distinctiv al unei persoane fizice/juridice şi care o deosebeşte de alte entități de acelaşi tip.

Obiect – obiect la care accesul este controlat, de exemplu un fişier, o aplicație, o zona de memorie principală unde se face asamblarea şi păstrarea datelor personale.

Perioada de activitate a certificatului – perioada dintre începutul şi sfârşitul validității unui certificat sau perioada dintre data de începere a validității certificatului şi momentul revocării sau suspendării lui

Politica de certificare – document sub forma unui set de reguli care sunt respectate strict de către o autoritate emitentă în timpul prestării serviciilor de certificare.

Politică de semnatura – soluții detaliate, tehnice şi organizaționale, care definesc metodele, scopul şi cerințele confirmării şi verificării unei semnaturi electronice, ale căror executare permite verificarea validității unei semnaturi.

Procedura de aplicat în situațiile de urgență - procedura alternativă la cea standard, care se execută la apariția unei situații de urgență.

Publicarea certificatelor şi a Listei de certificate Revocate – procedurile de distribuire a certificatelor emise şi a certificatelor revocate.

Punct de încredere – Autoritate de Certificare cu cea mai mare încredere, în care are încredere un Abonat sau o Entitate Parteneră. Un certificat al acestei autorități este primul certificat în fiecare cale de certificare creată de Abonat sau de Entitatea Parteneră. Alegerea punctului de încredere este de obicei impusă de politica de certificare care guvernează funcționarea entității care emite certificatul.

Revocarea unui certificat – definește procedurile privind revocarea unei perechi de chei valide (revocarea de certificat) în cazul în care accesul la perechea de chei trebuie restricționat pentru a preveni posibila utilizare a sa în

criptarea sau crearea de semnatura electronica. Un certificat revocat este plasat pe Lista de certificate Revocate (CRL).

Secret partajat – parte a unui secret criptografic, de ex. o cheie distribuită între n persoane de încredere (jetoane criptografice, de ex. carduri electronice) în aşa fel încât este nevoie de m părţi ale secretului (unde m<n) pentru a restaura cheia distribuită.

Semnatura electronica – transformarea criptografică a datelor pentru a permite atât verificarea originii şi integrităţii datelor de către destinatarul acestora cât şi protejarea expeditorului şi a destinatarului împotriva falsificării de către primitor; semnaturile electronice asimetrice pot fi generate de către o entitate prin folosirea unei chei private şi a unui algoritm asimetric, ex. RSA.

Sistem informatic – întreaga infrastructură, personal şi componente folosite pentru asamblarea, procesarea, depozitarea, transmiterea, publicarea, distribuirea şi managementul informaţiei.

Solicitant – Abonatul în perioada dintre trimiterea cererii către o Autoritate de Certificare până la încheierea procedurii de emitere a certificatului.

Sponsorul Abonatului – instituţia care în numele Abonatului suportă costurile financiare ale serviciilor de certificare prestate de autoritatea emitentă de certificate. Sponsorul este proprietarul certificatului.

Stările unei chei private – o cheie privată poate fi în una din următoarele trei stări fundamentale (conform standardului ISO/IEC 11770-1):

- **în aşteptarea activării (pregătită)** – cheia a fost deja generată dar nu est încă disponibilă pentru folosire;
- **activă** – cheia poate fi folosită în operaţiuni criptografice (de ex. pentru crearea de semnaturi electronice);
- **inactivă** – cheia poate fi folosită exclusiv pentru decriptare sau perechea ei publica pentru verificarea de semnaturi electronice.

Transformarea stării cheii – starea unei chei poate fi schimbată numai când apare una dintre următoarele transformări (în conformitatea cu ISO/IEC 11770-1):

- generarea – procesul de generare de chei; generarea de cheie trebuie să se realizeze în concordanţă cu procedurile acceptate; procesul poate include proceduri de testare cu scopul de a îmbunătăţi calitatea cheii;
- activarea – are ca rezultat devenirea validă a unei chei şi disponibilă pentru executarea de operaţii criptografice;
- dezactivarea – restrângerea unei chei; poate să apară la expirarea perioadei de validitate a cheii;
- reactivarea – permite folosirea în continuarea a unei chei aflata în starea de indisponibilitate pentru executarea de operaţii criptografice;
- distrugerea – are ca rezultat terminarea ciclului de viaţă al cheii; această noţiune se referă la distrugerea logică a cheii dar poate fi aplicată şi la distrugerea ei fizică.

Terţi de încredere (TTP) – instituţie sau reprezentantul său în care are încredere o entitate autentificată, o entitate care execută verificări sau alte entităţi din zona operaţiilor asociate cu securitatea şi autentificarea.

Furnizor de servicii de certificare – instituție de încredere (inclusiv dispozitivele hardware aflate sub controlul sau) care face parte dintre terții de încredere şi care furnizează servicii capabile să creeze, să semneze şi să emită certificate sau servicii de ne-repudiere.

Validarea certificatelor de cheie publică – verificarea stării unui certificat, care permite stabilirea dacă certificatul este revocat sau nu. Această problemă poate fi rezolvată pe baza CRL-ului sau printr-o cerere trimisă direct serverului OCSP.

Anexa 2: Acronime şi definiţii

CA	certification Authority
CP	certification Policy
CPS	certification Practice Statement
CRL	certificate Revocation List
DN	Distinguished Name
DSCS	Dispozitiv Securizat de Creare a Semnaturii
LRA	Local Registration Authority
OSCP	On-line certificate Status Protocol
PKI	Public Key Infrastructure
PRA	Primary Registration Authority
PSE	Personal Security Environment
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
TTP	Trusted Third Party

Anexa 3

Standardele şi recomandările internaționale referite în document

Recomandările Internet Engineering Task Force - http://www.ietf.org/rfc.html.

RFC 822 "Standard for the format of ARPA Internet text messages"

RFC 1778 „The String Representation of Standard Attribute Syntaxes"

RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

RFC 2560 „X.509 Internet Public Key Infrastructure Online certificate Status Protocol – OCSP"

RFC 3039 "Internet X.509 Public Key Infrastructure - Qualified certificates Profile "

RFC 3161 „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)"

RFC 3280 "Internet X.509 Public Key Infrastructure certificate and certificate Revocation List (CRL) Profile"

Recommendation International Telecommunication Union , seria X
http://www.itu.int/rec/T-REC-X/en

X.500 „Recommendation and International Standard that introduces the concepts of the Directory „

X.501 „Recommendation and International Standard that provides a number of different models for the Directory as a framework for the other ITU-T Recommendations în the X.500 series”

ITU-T X.509 v.3 „This Recommendation | International Standard defines a framework for public-key certificates and attribute certificates”

X.520 „This Recommendation | International Standard defines a number of attribute types and matching rules which may be found useful across a range of applications of the Directory”

Standardele PKCS ale RSA - http://www.rsasecurity.com/rsalabs/node.asp?id=2124

PKCS#7 Cryptographic Message Syntax Standard

PKCS#10 certification Request Syntax Standard

PKCS#12 Personal Information Exchange Syntax Standard

Standardele ISO - www.iso.org

ISO/IEC 11770-1 – Key management

ISO/IEC 13335 - Guidelines for Management of IT Security

ISO/IEC 17799 - Code of Practice for Information Security Management.

Standardele FIPS - http://csrc.nist.gov/publications/fips/index.html

FIPS 112 - Password usage

FIPS 140 – 2 Security Requirements for Cryptographic Modules

Common Criteria - http://www.commoncriteriaportal.org/

Standardele ETSI - http://www.etsi.org/

ETSI TS 101456 (Cerițele de Politică pentru Autoritățile de Certificare care emit certificate calificate)

Standardele CEN - http://www.cenorm.be/cenorm/index.htm

CEN CWA 14167 - Security Requirements for Trustworthy Systems Managing certificates for Electronic Signatures