S.C. DigiSign S.A.

Codul de practici şi proceduri

Versiunea 1.5

Data : 04-01-2010

Observaţii preliminare

Cererile de obţinere a permisiunii de reproducere a CPP (Codului de Practici şi Proceduri) al S.C. DigiSign S.A. (precum şi cele de copii de la S.C. DigiSign S.A.) trebuie adresate către:

S.C. DigiSign S.A.

Str. Virgil Madgearu nr 2-6, Sector 1, 014135, Bucuresti

Tel: +40-31-6201284

Fax: +40-31-6201286

e-mail: cpp@digisign.ro

1. Introducere

Acest document constituie Codul de Practici şi Proceduri (numit în continuare prescurtat şi CPP) al S.C. DigiSign S.A. Acest CPP descrie practicile si procedurile de lucru pe care autoritatea de certificare DigiSign S.A. ("AC") le utilizează în furnizarea serviciilor de certificare, care emite, administrează, revocă şi reînnoieşte certificatele în conformitate cu prevederile reglementărilor legale în materie, şi anume Legea nr. 455/2001 privind semnătura electronică, Hotărârea Guvernului nr. 1259/2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, cu modificările ulterioare şi Directiva 1999/93/EC a Parlamentului European şi al Consiliului European şi încheiată la 13 Decembrie 1999 privind stabilirea cadrului comunitar pentru semnătură electronică, cu modificările şi completările ulterioare.

1.1 Rezumat

Acest cod de practici şi proceduri se aplică companiei DigiSign S.A., ca Autoritate de Certificare (AC) şi ca Autoritate de Înregistrare (AI), precum şi oricăror AC-uri sau AI-uri aflate în relaţie de subordonate sau aflate în relaţie contractuală cu S.C. DigiSign S.A.

(a) Rolul CPP-ului DigiSign S.A.

Acest CPP prezintă şi explică practicile şi procedurile de lucru ale companiei DigiSign S.A., conținând printre altele:

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

(b) Informaţii referitore la certificate digitale

Specialiştii companiei DigiSign S.A. care au participat la realizarea Codului de Practici şi Proceduri pleacă de la premiza că cititorul are cunoştinţe generale despre semnătura digitală şi PKI. Dacă nu, DigiSign S.A. sfătuieşte cititorul să se documenteze în ceea ce priveşte folosirea infrastructurii de chei publice (*eng.* PKI). Informaţii generale şi pregătitoare sunt prezentate de către compania DigiSign S.A. la:

http://www.digisign.ro/

(c) Îndeplinirea standardelor în vigoare

Practicile amintite în acest CPP au fost proiectate pentru a satisface sau chiar a depăşi cerinţele standardelor general acceptate şi de dezvoltare a acestui domeniu şi a altor standarde ale industriei privind acţiunea AC-urilor.

Structura acestui CPP corespunde la modul general cu ***„Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”***, cunoscute ca RFC 3647.

1.1.1 Rezumatul politicii de certificare

S.C. DigiSign S.A. oferă certificate calificate DigiSign® pentru orice tip de utilizator, în limita legilor în vigoare.

Certificatele calificate DigiSign® pot fi utilizate pentru semnături digitale, criptare şi autentificare web, toate împreună sau separat (în funcţie de serviciul ales de beneficiar) ca dovadă a identităţii în orice tip de tranzacţii electronice. Certificatele furnizează siguranţa identităţii utilizatorului pe baza prezenţei fizice a acestuia în faţa unei persoane care îi confirmă identitatea, folosind cel puţin o formă de identificare recunoscută de autorităţi.

1.2 Sfera de aplicabilitate

Majoritatea utilizatorilor de certificate digitale furnizate de DigiSign S.A. sunt localizaţi în România.

1.2.1 Autorităţi de certificare

Termenul autoritate de certificare cuprinde toate entităţile care emit certificate respectând propriul CPP, care poate fi acelaşi pentru fiecare ACP, sau poate diferi de la un ACP la altul, în funcţie de scopul ACP-ului. Termenul "ACP" se referă la o subcategorie de emitenţi numite autorităţi de certificare primare (ACP), care se comportă ca rădăcini (*eng.* root). Fiecare ACP este o entitate DigiSign®. Subordonate ACP-ului sunt autorităţile de certificare, care emit certificate abonaţilor-utilizatori finali sau altor AC-uri. Toate ACP-urile DigiSign® sunt găzduite de centrul de procesare propriu, aflat pe teritoriul României, în locaţiile strict securizate.

1.2.2 Autorităţi de înregistrare

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

Toate AI-urile DigiSign® care asista ACP-urile DigiSign® la emiterea de certificate abonaţilor-utilizatori finali sunt găzduite în propriile locaţii securizate**.**

1.2.3 Utilizatorii finali

S.C. DigiSign S.A. oferă certificate calificate DigiSign® pentru orice tip de utilizatori, în condiţiile respectării legislaţiei în vigoare.

1.2.4 Aplicabilitate

Acest CPP se adresează tuturor participanţilor, incluzând DigiSign S.A., distribuitori, abonaţi şi alte părţi contractante. Acest CPP descrie practicile care guvernează utilizarea certificatelor calificate DigiSign®. Utilizatorilor de servicii DigiSign® li se permite să folosească certificate pentru aplicaţii de mare securitate care sunt descrise în prezentul CPP.

1.2.4.1 Aplicabilitatea vizată

Certificatele calificate DigiSign® destinate utilizatorilor permit terţilor, participanţi în procesul de comunicare electronică să verifice semnăturile digitale. Supusă legilor în vigoare, o semnătură digitală sau o tranzacţie interacţionând cu certificatul calificat DigiSign® va fi valid indiferent de locul în care certificatul calificat DigiSign® este emis sau de locul unde semnătura digitală a fost creată sau utilizată şi indiferent de locul unde AC-ul sau utilizatorul îşi desfăşoară activitatea.

1.2.4.2 Restricţii de aplicabilitate

În general, certificatele calificate DigiSign® au scopuri generale. Cerificatele calificate DigiSign® pot fi folosite la nivel global. Utilizarea certificatelor calificate DigiSign® nu este limitată la un anumit mediu de afaceri, cum ar fi un program pilot, un sistem de servicii financiare sau un mediu de piaţa virtuală. S.C. DigiSign S.A. sau ceilalţi participanţi nu sunt responsabili pentru monitorizarea sau impunerea vreunei restricţii în aceste medii.

Cu toate acestea, anumite certificate calificate DigiSign® au funcţii limitate. De exemplu, certificatele ACP nu pot fi utilizate pentru alte funcţii decât cele de ACP. Mai mult, certificatele pentru client se supun aplicaţiilor clientului şi nu vor fi folosite ca certificate de server. În plus, certificatele de administrator nu vor fi utilizate decât pentru a executa funcţiile de administrator.

De asemenea, în ceea ce priveşte certificatele calificate DigiSign®, care respectă standardul X.509 v3 în privinţa certificatelor şi X.509 v2 în privinţa listei certificatelor revocate - CRL (derivat din RFC 3280 – ***„Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile”***), extensia de folosire a cheii limitează scopurile tehnice pentru care poate fi utilizată o cheie privată corespunzătoare cheii publice dintr-un certificat. În plus, certificatele de utilizator final nu pot fi utilizate ca certificate AC. Această restricţie este confirmată de absenta unei extensii.

În general, certificatele pot fi utilizate doar cu extensia folosită la generarea lor, concordând cu legea aplicabilă, şi, particular vorbind, pot fi utilizate doar la extensia permisă de legile aplicabile.

1.3 Detalii de contact

1.3.1 Organizarea şi administrarea CPP-ului

Personalul care administrează acest CPP este constituit în grupul de dezvoltare a practicilor şi procedurilor DigiSign S.A.

Întrebările cu privire la grupul de dezvoltare a practicilor şi procedurilor companiei DigiSign S.A. ar trebui adresate după cum urmează:

S.C. DigiSign S.A.

Str. Virgil Madgearu nr 2-6, Sector 1, 014135, Bucuresti

Tel: +40-31-6201284

Fax: +40-31-6201286

e-mail: cpp@digisign.ro

În atenția: Practici de Dezvoltare – CPP

1.3.2 Persoană de contact

Adresați întrebări despre acest CPP la următoarea adresă:

S.C. DigiSign S.A.

Str. Virgil Madgearu nr 2-6, Sector 1, 014135, Bucuresti

Tel: +40-31-6201284

Fax: +40-31-6201286

e-mail: cpp@digisign.ro

2. Dispoziţii generale

2.1 Obligaţii

2.1.1 Obligaţiile Autorităţii de Certificare - AC

S.C. DigiSign S.A. face eforturi continue ca să asigure buna legătura dintre serviciile oferite utilizatorilor şi abonaţii la aceste servicii, ambii constituindu-se în părţi contractante, obligaţiile ambelor părţi fiind stipulate clar şi fără echivoc în cadrul contractului dintre părţi în spiritul prezentului CPP.

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

11. Crearea unui document care să reflecte clar modalităţile de lucru, procedurile aplicabile şi aplicate, politica generală a firmei, obligaţiile şi drepturile părţilor contractante, etc. - CPP (Codul de Practici şi Proceduri) şi afişarea lui în mod public (pe Internet) după ce a fost aprobat de persoanele responsabile din cadrul AC-ului;
22. Modul de desfăşurare a activităţii AC-ului să se conformeze strict cu prevederile CPP-ului aprobat;
33. Modalitatea de punere în practică a CPP-ului şi a Politicilor de Certificare ale AC-ului să se bazeze pe o infrastructura (de comunicaţii, software şi hardware) fiabilă, capabilă în orice moment de a garanta buna desfăşurare a activităţii AC-ului conform cu politica de funcţionare 24x7 impusă nu numai de legile româneşti în vigoare privind Autorităţile de Certificare ce emit certificate calificate, dar şi de realităţile lumii contemporane în ceea ce priveşte afacerile desfăşurate pe Internet;
44. Garantarea faptului că cererile de emitere de certificate sunt procesate (în sensul identificării persoanei numai pe baza modalităţilor puse la dispoziţie de legile române în vigoare) numai de o AI aflată în legătură contractuală cu AC-ul emitent de certificate (şi căruia i se subordonează), şi care la rândul ei se conformează cadrului general stabilit de prezentul CPP, în strânsă legătură şi cu documentul ce statutează Politica de Certificare a AC-ului;
5. Garantarea faptului că activitatea AI-ului pe linia identificării persoanelor ce se înregistrează în vederea obţinerii unui certificat digital calificat se desfăşoară în litera şi spiritul Legii nr. 677/ 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;

56. Garantarea faptului că informaţiile incluse în certificate sunt valide şi conform realităţii la momentul aprobării certificatului, precum şi garantarea menţinerii conform Legii 455/2001 a actelor ce fac dovada identităţii persoanelor înregistrate în vederea eliberării certificatului calificat;
67. Garantarea aducerii la cunoştinţa utilizatorilor a obligaţiilor pe care le au în concordanţă cu acest CPP, prin prisma faptului că sunt posesori şi virtual utilizatori ai certificatelor digitale calificate, precum şi informarea acestora asupra riscului la care se supun prin nerespectarea acestor obligaţii;
78. Revocarea (sau suspendarea – după caz) a certificatelor acelor utilizatori despre care s-a stabilit (sau există dubii) că au acţionat contrar obligaţiilor ce revin utilizatorilor, aşa cum se desprind ele din acest CPP, cu obligativitatea AC-ului de a anunţa utilizatorul despre măsura luată;
89. Serviciile de înregistrare în vederea emiterii de certificate şi de ridicare a certificatelor în urma aprobării acestora, servicii ce sunt destinate utilizatorului final trebuie să fie furnizate exclusiv prin mijloace electronice, bazate pe o infrastructură care să permită rularea acestora pe Internet (iar în cazuri particulare pe Intranet), cu obligativitatea AC-ului de a menţine un registru de evidenţă a certificatelor emise de către toate ACP-urile subordonate, registru ce trebuie actualizat dinamic astfel încât el să reflecte situaţia la zi a certificatelor emise către abonaţi;

2.1.2 Obligaţiile Autorităţii de Înregistrare - AI

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

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

1• Distribuirea de chei si/sau certificate către abonaţi;
2• Trimiterea de cereri către AC pentru eliberarea, suspendarea, revocarea sau reînnoirea certificatelor;
3• Verificarea prealabila a datelor furnizate de abonaţi pentru aceste cereri, conform cerinţelor din CPP;

4• Asigurarea faptului ca PIN-ul si cheia privată ce urmează să se distribuie către abonat nu sunt interceptate de către terţe părţi;
5• Transmiterea unui contract („Acordul Părţilor") ce urmează a fi semnat, către fiecare utilizator ce urmează a fi deţinătorul unui certificat.

2.1.3 Obligaţiile utilizatorului

Serviciile de certificare efectuate de către S.C. DigiSign S.A. apar la:

http://www.digisign.ro/registru/ .

Prestarea în bune condiţiuni a serviciilor respective presupune ca solicitanţii certificatelor să furnizeze informaţii complete şi precise în cererile pentru certificate şi să-şi manifeste acceptul faţă de serviciu, ca o condiţie de obţinere a certificatului.

Efectuarea respectivului serviciu pune în practică obligaţii specifice care apar în CPP pentru abonaţii DigiSign S.A. Serviciile cer abonaţilor să-şi folosească certificatele în concordanţă cu CPP § 1.2.2. Cer, de asemenea, abonaţilor să-şi protejeze cheile private în concordanţă cu CPP § 6.1 - §6.4. Sub regimul serviciilor, dacă un utilizator descoperă sau are motive să creadă că cheia sa privată sau datele de activare a protecţiei cheii private au fost compromise, sau alte informaţii cuprinse în certificat sunt incorecte sau s-au schimbat, trebuie în mod prompt :

- Să anunţe DigiSign S.A. care a aprobat cererea utilizatorului pentru certificat, sau o AC sau o AI, în concordanţă cu CPP § 4.4.1 şi cererea de revocare a certificatului în concordanţă cu CPP § 3.4;
- Sa înceteze utilizarea cheii private din momentul sesizarii compromiterii acesteia.

Utilizarea acestor servicii puse la dispoziţie de către DigiSign S.A. abonaţilor presupune ca aceştia să sisteze utilizarea cheii private la finalul perioadei de valabilitate a acestora, conform CPP § 6.3.2.

2.1.4 Obligaţiile părţilor contractante

Acordul părţilor contractante privind serviciul de furnizare de certificate digitale de către S.C. DigiSign S.A. poate fi consultat la:

http://www.digisign.ro/uploads/contract.pdf .

Acordurile părţilor contractante confirma că înainte de orice act de suport, părţile contractante trebuie să evalueze în mod independent folosirea certificatului pentru orice scop dat şi să determine că certificatul va fi folosit într-un scop corespunzător. Acesta confirma că DigiSign S.A., d.p.d.v. al AC şi AI, nu este responsabilă pentru folosirea necorespunzătoare a certificatului. Acordul părţilor contractante prevede în mod expres că acestea nu trebuie să folosească certificatele dincolo de limitele stipulate în CPP § 1.2.4.2.

Acordurile părţilor contractante confirma mai departe că părţile trebuie să utilizeze un software şi/sau hardware adecvat ca să execute verificarea semnăturii digitale sau alte operaţiuni criptografice pe care le doresc, ca o condiţie de siguranţă a certificatelor în legătură cu fiecare astfel de operaţie. Astfel de operaţiuni includ identificarea unui lanţ de certificate şi verificarea semnăturilor digitale a tuturor certificatelor din lanţul respectiv. Sub regimul acestor acorduri, părţile contractante nu trebuie să se bazeze pe un certificat decât dacă aceste proceduri de verificare au fost făcute cu succes.

Acordurile părţilor contractante obligă de asemenea părţile să verifice statutul certificatului pe care doresc să se bazeze, cât şi a tuturor certificatelor din lanţul de certificate. Dacă oricare dintre certificatele din lanţul de certificate a fost revocat, în conformitate cu acordurile părţilor contractante, părţile contractante nu trebuie să se bazeze pe certificatul utilizatorului final sau pe alte certificate revocate din lanţul de certificate. In cazul in care partea contractanta a fost informata de compromiterea cheii private a unei autoritati din lantul de certificare, aceasta se obliga sa sa se asigure ca utilizatorii finali ai partii contractante nu vor mai folosi certificatele.

În încheiere, acordul părților contractante prevede că acceptarea termenilor este o condiție pentru folosirea de certificate calificate. Utilizatorii părți contractante cu DigiSign S.A., care sunt de altfel şi abonați, sunt de acord să fie legați de condițiile părților contractante din aceasta secțiune, atunci când au acceptat acest serviciu.

Acordurile părților contractante confirma că dacă toate verificările descrise mai sus au fost făcute cu succes, părțile contractante sunt îndreptățite să se bazeze pe certificat. Dacă circumstanțele indică nevoia de asigurări adiționale, părțile contractante trebuie să obțină astfel de asigurări, pentru un grad sporit de siguranță.

2.1.5 Obligaţiile S.C. DigiSign S.A.

DigiSign S.A. este responsabilă cu funcțiile de depozitare şi afişare în mod public a certificatelor digitale emise de AC-urile proprii. DigiSign S.A. publică în registrul propriu certificatele pe care le emite.

În cazul revocării unui certificat, DigiSign S.A. publică o înştiinţare a revocării în registrul propriu. DigiSign S.A. emite liste de revocare a certificatelor pentru propriile AC-uri.

2.2 Responsabilitate

2.2.1 Responsabilitatea Autorităţii de Certificare - AC

Răspunderea furnizorilor de servicii de certificare este reglementată de lege in sensul ca, în art. 41 din Legea nr. 455/2001 privind semnătura electronică, se prevede ca furnizorul de servicii de certificare, care eliberează certificate prezentate ca fiind calificate sau care garantează asemenea certificate, este răspunzător pentru prejudiciul adus oricărei persoane care îşi întemeiază conduita pe efectele juridice ale respectivelor certificate: a) în ceea ce priveşte exactitatea, în momentul eliberării certificatului, a tuturor informațiilor pe care le conține; b) în ceea ce priveşte asigurarea că, în momentul eliberării certificatului, semnatarul identificat în cuprinsul acestuia deținea datele de generare a semnăturii corespunzătoare datelor de verificare a semnăturii menționate în respectivul certificat; c) în ceea ce priveşte asigurarea că datele de generare a semnăturii corespund datelor de verificare a semnăturii, în cazul în care furnizorul de servicii de certificare le generează pe amândouă; d) în ceea ce priveşte suspendarea sau revocarea certificatului, în

cazurile şi cu respectarea condiţiilor prevăzute la art. 24 alin. (1) şi (2); e) în privinţa îndeplinirii tuturor obligaţiilor prevăzute la art. 13-17 şi la art. 19-22, cu excepţia cazurilor în care furnizorul de servicii de certificare probează că, deşi a depus diligenţa necesară, nu a putut împiedica producerea prejudiciului.

De asemenea**,** furnizorul de servicii de certificare poate să indice în cuprinsul unui certificat calificat restricţii ale utilizării acestuia, precum şi limite ale valorii operaţiunilor pentru care acesta poate fi utilizat, cu condiţia ca respectivele restricţii să poată fi cunoscute de terţi. Furnizorul de servicii de certificare nu va fi răspunzător pentru prejudiciile rezultând din utilizarea unui certificat calificat cu încălcarea restricţiilor prevăzute în cuprinsul acestuia. (art. 42 din Legea nr. 455/2001 privind semnătura electronică)

2.2.1.1 Garanţiile Autorităţii de Certificare - AC

Furnizorul de servicii de certificare calificată trebuie să dispună de resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfăşurării activităţilor legate de certificarea semnăturilor electronice. In acest sens, asigurarea se realizează fie prin subscrierea unei polite de asigurare la o societate de asigurări, fie prin intermediul unei scrisori de garanţie din partea unei instituţii financiare de specialitate, fie printr-o altă modalitate stabilită prin decizie a autorităţii de reglementare şi supraveghere specializate în domeniu. Suma asigurată şi suma acoperita prin scrisoare de garanţie sunt stabilite de către Ministerul Comunicaţiilor si Tehnologiei Informaţiei, in calitate de autoritate de reglementare si supraveghere specializată în domeniu. (art. 22 din Legea nr. 455/2001 privind semnătura electronică).

Serviciile DigiSign S.A. includ de asemenea o garanţie pentru abonaţi după cum urmează:

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

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

- Toate informaţiile din sau incorporate într-un astfel de certificat, excepţie făcând informaţiile neverificate despre utilizator, sunt precise;
- În cazul certificatelor apărute în registrul DigiSign S.A., certificatul a fost emis pentru o persoană fizică sau companie şi utilizatorul a acceptat certificatul în concordanţă cu CPP § 4.3;
- Entităţile care aprobă cererile pentru certificat şi emit certificate au respectat acest CPP atunci când au emis certificatele.

2.2.1.2 Forţa majoră

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

2.2.2 Responsabilitatea Autorităţii de Înregistrare - AI

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

2.2.3 Responsabilitatea utilizatorului

2.2.3.1 Garanţiile utilizatorului

Serviciile DigiSign S.A. cer abonaţilor să garanteze că:

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

2.2.3.2 Compromiterea cheii private

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

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

2.2.4 Responsabilitatea părţilor contractante

Părţile contractante admit că au informaţii suficiente pentru a lua o decizie în măsura în care au ales să se bazeze pe informaţiile dintr-un certificat, că sunt singurii responsabili pentru decizia de a se baza sau nu pe astfel de informaţii, şi că vor suporta consecinţele legale în cazul nerespectării obligaţiilor de către părţi, conform CPP § 2.1.4.

2.3 Responsabilităţi financiare

2.3.1 Despăgubirea de către abonaţi

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

- Falsitate sau relatare greşită în cererea pentru certificate;
- Relatarea greşită a unei informaţii importante în cererea pentru certificat, dacă relatarea greşită sau omisiunea a fost făcută din neglijenţă sau cu intenţia de a înşela una dintre părţi;
- Neprotejarea cheii private sau neluarea măsurilor de protecţie necesare prevenirii, compromiterii, pierderii, dezvăluirii, modificării sau folosirii neautorizate a cheii private a utilizatorului;
- Utilizatorul a folosit un nume (inclusiv un nume comun, nume de domeniu sau adresa de e-mail), care încalcă drepturile de proprietate intelectuală a unui terţ.

2.3.2 Procese administrative

DigiSign S.A. are suficiente resurse financiare ca să-şi menţină operaţiunile şi să-şi execute îndatoririle şi trebuie să suporte riscul răspunderii faţă cealaltă parte contractantă, conform art. 22 din Legea nr. 455/2001 privind semnătura electronică.

2.4 Interpretare şi sancţionare

2.4.1 Legea aplicabilă

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

2.4.2 Proceduri privind soluţionarea litigiilor

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

2.5 Taxe

2.5.1 Taxe de emitere sau reînnoire a certificatului

DigiSign S.A. este îndreptăţită să taxeze utilizatorul final pentru emiterea, administrarea şi reînnoirea certificatelor.

2.5.2 Taxe pentru alte servicii

DigiSign S.A. este îndreptăţită să perceapă taxe pentru serviciile conexe (ex. Servicii de implementare, consultanţă, şcolarizare, etc.) daca acestea fac obiectul acordului dintre parti.

2.5.3 Politica de restituire

Politicile de restituire ale companiei DigiSign S.A. (reproduse la http://www.digisign.ro/registru/restituire/) sunt:

DigiSign S.A. aderă şi susţine procedurile riguroase şi politicile privind operarea şi emiterea certificatelor. Cu toate acestea, dacă un utilizator nu este satisfăcut complet de certificatul emis pentru el, poate cere DigiSign S.A. să revoce certificatul în treizeci (30) de zile de la emitere şi să restituie utilizatorului taxa. În perioada iniţială de treizeci (30) de zile un utilizator poate cere companiei DigiSign S.A. să revoce certificatul şi să-i fie restituită taxa dacă DigiSign S.A. nu respectă garanţia sau orice altă obligaţie impusă de CPP privind utilizatorul sau certificatul acestuia. După ce DigiSign S.A. revocă certificatul, va credita imediat contul cărţii de credit a utilizatorului (dacă certificatul a fost plătit cu carte de credit) sau va rambursa utilizatorului prin aceeasi metoda prin care a fost facuta plata de catre utilizator suma totală a taxelor plătite pentru certificat. Pentru a cere o restituire vă rugăm să sunaţi la departamentul de relaţii cu clienţii. Această politică de restituire nu este o măsura exclusivă şi nu limitează alte măsuri care pot fi disponibile abonaţilor.

2.6 Publicarea şi înregistrarea informaţiilor

2.6.1 Publicarea informaţiilor despre AC

DigiSign S.A. publică anumite informaţii despre AC în registrul de pe site-ul web al DigiSign S.A. la http://www.digisign.ro/registru/, aşa cum se detaliază în continuare.

DigiSign S.A. publică acest CPP, serviciile şi acordurile părţilor contractante pe site-ului web al S.C. DigiSign S.A.

DigiSign S.A. publică statutul informaţiilor privind certificatele.

2.6.2 Frecvenţa publicării

Actualizările făcute la acest CPP sunt publicate în concordanţă cu CPP § 8. Actualizările serviciilor furnizate de către DigiSign S.A. sunt publicate dacă este necesar. Certificatele sunt publicate după emitere.

2.6.3 Controlul accesului la informaţii

Informaţiile publicate pe site-ului web al S.C. DigiSign S.A. sunt informaţii publice. Accesul doar pentru a citi aceste informaţii nu este restricţionat. Compania DigiSign S.A. solicită persoanelor să accepte acordul părţilor contractante sau acordul de utilizare al listei de revocare a certificatelor ca o condiţie pentru a putea accesa certificatele, statutul informaţiilor privind certificatele sau listele de revocare a certificatelor. S.C. DigiSign S.A. a implementat măsuri de securitate logică şi fizică pentru a preveni intrarea persoanelor neautorizate care ar putea adăuga, şterge sau modifica registrul.

2.7 Audit de conformitate

DigiSign S.A. va avea dreptul să execute revizuiri şi investigaţii ca să asigure credibilitatea DigiSign S.A. care includ, dar nu se limitează la:

- DigiSign S.A. sau reprezentanții autorizați de ea vor avea dreptul să realizeze propriile "Revizuiri suplimentare privind administrarea riscului", pe baza constatărilor incomplete sau excepționale într-un audit de conformitate sau ca o parte a procesului de risc total de management în cursul normal al activității.

DigiSign S.A. sau reprezentanții autorizați de ea vor avea dreptul să delege executări de verificare, revizuiri sau investigații unui terț - firma de audit. Entitățile care se supun unei verificări, revizuiri sau investigații cooperează cu DigiSign S.A. şi cu personalul care execută verificarea, revizuirea sau investigarea..

2.7.1 Frecvența auditului de conformitate

Auditul de conformitate este realizat anual, iar costurile sunt suportate de entitatea care este supusă verificării.

2.7.2 Identitatea/ calificarea verificatorului

Auditul de conformitate cu politicile şi practicile DigiSign S.A. este realizat de o firmă publică ce:

- demonstrează competența în domeniul IT&C în general şi pe linia PKI în special;
- este recunoscută ca firmă de audit şi consultanță.

În cazul S.C. DigiSign S.A. auditul este asigurat de firmele KPMG, TÜV si Certlab

2.7.3 Relația auditorului cu partea verificată

Auditul de conformitate cu politicile şi practicile DigiSign S.A. este realizat de o firmă de audit publică, independentă de DigiSign S.A.

Scopul auditului DigiSign S.A. include controalele mediului AC, AI şi operațiunile de administrare a cheii.

2.7.4 Acţiuni acceptate ca rezultat al deficienţei

În cazul auditului de conformitate cu politicile şi practicile DigiSign S.A., pot rezulta excepţii şi neconformităţi semnificative, în ceea ce priveşte delimitarea acţiunilor care vor avea loc. Delimitarea este făcută de administraţia companiei DigiSign S.A. cu acceptul auditorului. Administraţia DigiSign S.A. este responsabilă cu dezvoltarea şi implementarea unui plan activ de implementare de acţiuni preventive şi corective. Dacă DigiSign S.A. consideră că astfel de excepţii sau neconformităţi pun în pericol securitatea sau integritatea, va fi dezvoltat un plan de rectificare în 30 de zile şi va fi implementat într-o perioadă de timp eficientă. În cazul neconformităţilor mai puţin grave, administraţia companiei DigiSign S.A. le va evalua şi va determina acţiunile preventive şi corective corespunzătoare.

2.7.5 Comunicarea rezultatelor

Rezultatele auditului de conformitate cu politicile şi practicile companiei DigiSign S.A. vor fi puse la dispoziţia administraţiei DigiSign S.A.

2.8 Confidenţialitate

DigiSign S.A. a implementat politica de confidenţialitate, care poate fi găsită la: http://www.digisign.ro/ro/footer/politica_de_confidentialitate

2.8.1 Tipuri de informaţii confidenţiale şi private

Următoarele rapoarte se supun CPP § 2.8.2, şi sunt confidenţiale şi private ("Informaţii confidenţiale/private"):

- Rapoartele cererilor pentru certificate (se supun CPP § 2.8.2),
- Rapoarte tranzacţionale (atât rapoarte totale, cât şi procesul de audit al tranzacţiilor),
- Rapoartele de audit DigiSign S.A., create de DigiSign S.A. sau de auditorii lor (interni sau externi).
- Planurile în caz de incidente şi pentru recuperarea după dezastru,
- Măsuri de securitate care controlează operaţiunile de hardware şi software ale DigiSign S.A. şi administrarea serviciilor pentru certificat şi serviciile destinate înscrierii.

2.8.2 Dezvăluirea informaţiilor către persoanele oficiale

Dezvăluirea informaţiilor confidenţiale de către DigiSign S.A. se va face numai în temeiul legii române în vigoare.

2.9 Drepturi de proprietate intelectuală

2.9.1 Drepturi de proprietate asupra informaţiilor privind certificatele şi revocarea lor

DigiSign S.A. deţine toate drepturile de proprietate intelectuală asupra certificatelor calificate emise de aceasta. Reproducerea certificatelor se poate face cu acordul exclusiv al DigiSign S.A., care se bucura de toate drepturile conferite de dreptul acestuia de autor al operei create, in virtutea Legii nr. 8/1996 privind dreptul de autor si drepturile conexe, cu modificările si completările ulterioare..

2.9.2 Drepturi de proprietate asupra numelor

Solicitantul de certificat păstrează toate drepturile pe care le are în ceea ce priveşte orice marcă comercială, marca de serviciu sau numele mărcii conţinute în orice solicitare pentru certificate, precum şi numele de utilizator din orice certificat emis unui solicitant.

2.9.3 Drepturi de proprietate asupra cheilor

Rădăcina cheilor criptografice folosite de DigiSign S.A. şi cea a certificatelor care o conţin, incluzând toate cheile publice AC şi certificatele auto-semnate, sunt proprietate a DigiSign S.A. În încheiere, fără limitarea anterioară a majorităţii, părţile secrete ale perechilor de chei a AC sunt proprietate a AC-ului, iar AC-ul deţine toate drepturile de proprietate intelectuală în şi pentru aceste părţi secrete.

3. Identificare şi autentificare

3.1 Înregistrarea inițiala

3.1.1 Tipuri de nume

Certificatele de AC ale DigiSign S.A. conţin nume caracteristice **X.501** (cunoscut ca standard **ISO/IEC 9594-2**) în câmpurile emiţătorului şi subiectului. Numele caracteristice ale AC-ului DigiSign S.A. constau în componentele specificate în tabelul 2 de mai jos.

Simbol	*Valoare*
Țara (C) =	"RO " sau nu este folosit
Compania (O) =	DigiSign S.A.
Element de organizație (OU) =	Certificatele AC-ului DigiSign S.A. pot conține multiple simboluri OU. Astfel de simboluri pot conține unul sau mai multe dintre punctele următoare: • Numele AC-ului • O declarație referitoare la condițiile de utilizare a certificatului, din Acordul Părților Contractante şi • O înștiințare privind drepturile de autor.
Județ/Sector (S) =	Nu se utilizează.
Localitate (L) =	Nu se utilizează.
Nume (CN) =	Acest simbol include numele AC-ului (dacă numele AC-ului nu este specificat într-un atribut OU) sau nu este folosit.

Tabelul 2 – Atribute „Distinguished Name" în certificatele de AC

Certificatele pentru abonați-utilizatori finali conțin un nume caracteristic X.501 în câmpul de nume principal şi conține componentele specificate în tabelul 3 de mai jos

Simbol	*Importanţa(Valoare)*
Ţara (C) =	"RO" sau nu este folosit
Companie (O) =	Simbolul companiei este utilizat după cum urmează: • "DigiSign S.A." pentru certificatele utilizatorilor care nu sunt afiliaţi unei organizaţii • Numele organizaţiei utilizatorului pentru certificatele individuale ale utilizatorilor afiliaţi unei organizaţii
Element de organizaţie (OU) =	Certificatele DigiSign S.A. pentru utilizatorii finali pot conţine multiple atribute OU. Aceste atribute pot conţine unul sau mai multe din punctele următoare: • Element de organizaţie pentru utilizator (pentru certificatele companiei sau pentru utilizatorii afiliaţi unei organizaţii) • O declaraţie referitoare la condiţiile de utilizare a certificatului din acordul părţilor contractante • O înştiinţare privind drepturile de autor • "Autentificat de DigiSign S.A.." în certificatele ale căror aplicaţii au fost autentificate de DigiSign S.A. • Text care să descrie tipul certificatului.
Judeţ/Sector (S) =	Indica judeţul/sectorul utilizatorului sau nu sunt utilizate.
Localitate (L) =	Indica localitatea utilizatorului sau nu sunt utilizate.
Nume (CN) =	Acest simbol include: • Nume (pentru certificatele individuale). • Denumirea companiei (pentru certificatele achiziţionate în numele companiei) • OCSP Responder Name (pentru OCSP Responder Certificates) • Numele de domeniu (pentru certificatele de

Simbol	*Importanţa(Valoare)*
	server)
E-Mail Address (E) =	Adresa de e-mail a utilizatorului

Tabelul 3 – Atribute „Distinguished Name" în certificatele utilizatorilor finali

Numele (CN) = este o componentă pentru „distinguished name" în cadrul certificatelor pentru utilizatorii finali, care trebuieşte a fi verificată şi validată de o AI în cazul certificatelor calificate

Importanţa numelui inclus în numele caracteristic principal al certificatului individual rezidă din faptul că acesta reprezintă numele general acceptat al persoanei fizice.

3.1.2 Necesitatea ca numele să aibă sens

Certificatele calificate DigiSign®, care sunt în fapt certificatele utilizatorului final trebuie să conţină nume uşor de înţeles, permiţând determinarea identităţii persoanei fizice ca subiect al certificatului. .

Certificatele AC-ului DigiSign S.A. conţin nume uşor de înţeles, permiţând determinarea identităţii AC-ului ca subiect al certificatului.

3.1.3 Unicitatea numelor

DigiSign S.A. permite ca numele sau combinatia de nume si alte elemente ale subiecţilor sa nu fie unice în cadrul domeniului unui AC.

3.1.4 Procedura care se aplică în litigiile ce au ca obiect dreptul la nume

Solicitanţilor de certificate li se interzice utilizarea, în cererile pentru certificate, a numelor care încalcă dreptul de proprietate al altor persoane. Oricum, compania DigiSign S.A. nu verifică dacă un solicitant are drepturi de proprietate intelectuală pentru numele care apare în cererea pentru certificat şi nici nu arbitrează, mediază sau rezolvă disputele în ceea ce priveşte proprietatea asupra numelui de domeniu, a

mărcii comerciale sau a mărcii de serviciu. DigiSign S.A. este îndreptăţită să înlocuiască, fără a răspunde faţă de solicitantul certificatului, să respingă sau să suspende orice cerere pentru certificat, în cazul unui litigiu.

3.1.5 Metode pentru a dovedi posesia cheii private

DigiSign S.A. verifică posesia cheii private a solicitantului de certificat prin utilizarea unei cereri de certificat semnată digital, în conformitate cu standardul PKCS #10, sau altă demonstraţie asemănătoare d.p.d.v. criptografic sau altă metodă aprobată de DigiSign S.A.

În cazul în care o pereche de chei este generată de DigiSign S.A., în numele utilizatorului (ex: acolo unde cheile deja generate sunt plasate pe smart card-uri), această cerere nu este aplicabilă.

3.1.6 Autentificarea identităţii companiei

Pentru cererile de certificate de AC sunt create CSR-uri pentru semnarea perechilor de chei de către cheia de root a DigiSign S.A., iar cererile sunt procesate şi aprobate de personalul autorizat al DigiSign S.A., folosind un proces controlat care cere participarea mai multor angajaţi de încredere ai companiei DigiSign S.A..

3.1.7 Autentificarea identităţii persoanelor fizice

Pentru certificatele individuale (în numele propriei AI care deserveşte AC-ul), S.C. DigiSign S.A. confirmă că:

- Solicitantul certificatului este persoana identificată în cererea pentru certificate;
- Solicitantul certificatului păstrează legal cheia privată corespunzătoare cheii publice listată în certificate, în concordanţă cu CPP-ul şi legile româneşti în vigoare,
- Informaţiile care apar în certificat sunt corecte sau au fost corecte la momentul aprobării certificatului

În plus, DigiSign S.A. desfăşoară şi alte proceduri mult mai detaliate, descrise mai jos, pentru certificatele calificate DigiSign®.

3.1.8 Certificate calificate DigiSign®

Autentificarea cererilor pentru certificatele calificate DigiSign® se bazează pe prezența fizică a solicitantului în față unui reprezentant autorizat al companiei DigiSign S.A., notar public, sau alte persoane oficiale care se supun jurisdicţiei DigiSign S.A. Agentul, notarul sau altă persoană oficială verifică identitatea solicitantului pe baza unui act de identitate recunoscut şi emis de o instituție, cum ar fi cartea (buletinul) de identitate, pașaportul sau o alta legitimație de identificare, toate acestea fiind însoțite şi de o declarație care să confirme identitatea solicitantului de certificate calificate.

3.2 Înlocuirea şi înnoirea

Înainte de expirarea termenului legal de valabilitate – un an – a unui certificat al utilizatorului, acesta trebuie să obțină un nou certificat pentru a menține continuitatea utilizării certificatului. DigiSign S.A. solicită ca utilizatorul să genereze o nouă pereche de chei pentru a înlocui perechea de chei expirată (definit tehnic "înlocuire").

În general, "înlocuirea" este descrisă ca "reînnoire a certificatului," punând accent pe faptul că vechiul certificat a fost înlocuit cu unul nou şi fără să scoată în evidență dacă a fost generată sau nu o nouă pereche de chei. Pentru certificatele calificate DigiSign, acest titlu nu este important pentru că o nouă pereche de chei este întotdeauna generată, ca parte a procesului de reînnoire a certificatului utilizatorului final.

Clase şi tipuri de certificate	*Cerințe privind reînnoirea şi înlocuirea*
Certificate	Utilizatorul nu are o opțiune care să îi permită trimiterea unei

Clase şi tipuri de certificate	*Cerinţe privind reînnoirea şi înlocuirea*
calificate	perechi de chei deja existente pentru a fi "reînnoită". În consecinţă, procesul de reînnoire constă în generarea altei perechi de chei care să corespundă unui certificat cu aceleaşi date ca certificatul expirat.
Certificate AC	Reînnoirea certificatelor AC este permisă atât timp cât durata cumulată de funcţionare a perechii de chei AC nu depăşeşte durata maximă de funcţionare specificată în CPP § 6.3.2. AC-urile DigiSign S.A. pot fi înlocuite în concordanţă cu CPP § 4.7.

Tabelul 4 – Condiţii de reînnoire şi înlocuire a certificatelor

3.2.1 Reînnoirea şi înlocuirea certificatelor utilizatorilor finali

Dacă nu au fost revocate, certificatele abonaţilor pot fi înlocuite în concordanţă cu tabelul 5 de mai jos.

Perioada	*Cerinţa*
Cu 30 de zile înainte de expirarea certificatului	În cadrul perioadei specificate, utilizatorii pot consulta si utiliza procedura de reinnoire a certificatelor. Procedura este publicata pe site-ul Digisign, la Obtinere/Reinnoire certificate calificate

Tabelul 5 –Condiţii privind înlocuirea şi reînnoirea certificatelor utilizatorilor finali

3.2.2 Înlocuirea şi reînnoirea certificatelor de AC

Cheile autorităţilor de certificare subordonate DigiSign S.A. pot fi înlocuite periodic, conform CPP § 4.7.

Certificatele de AC ce sunt subordonate DigiSign S.A. pot fi reînnoite respectând parametrii specificaţi în CPP la punctul § 6.3.2. De exemplu, dacă un certificat de AC a fost emis iniţial pe o perioadă de 10 ani, se poate reînnoi în perioada de valabilitate a perechii de chei a AC-ului pentru o perioadă de 20 de ani, atingând perioada de valabilitate maximă de 30 de ani. Reînnoirea certificatului de AC nu este permisă după expirarea lui.

3.3 Înlocuire după revocare

Nu este permisă înlocuirea după revocare, în cazul în care:

- Revocarea a avut loc pentru că certificatul a fost emis unei alte persoane decât celei numite drept subiect al certificatului,
- Certificatul a fost emis fără autorizarea persoanei numite drept subiect al certificatului,
- Entitatea care aprobă cererea utilizatorului de certificat descoperă sau are motiv să creadă că anumite informaţii înscrise în cererea pentru certificate sunt false.

Subiect al paragrafului menţionat înainte, certificatele utilizatorilor care au fost revocate pot fi înlocuite în concordanţă cu tabelul 6 de mai jos.

Perioada de timp	*Cerinţe*
Înainte de expirarea certificatului	Pentru înlocuirea unui certificat individual, după revocarea acestuia, DigiSign S.A. verifică dacă persoana care doreşte înlocuirea certificatului este de fapt utilizatorul iniţial prin folosirea cerinţelor de validare a unei cereri originale de certificat pentru a înlocui certificatul după revocare. Astfel de certificate conţin acelaşi nume al subiectului ca şi numele care apare pe certificatul care este înlocuit.
După expirarea certificatului	În această situaţie se procedează ca în cazul unei cereri primare de certificat.

Tabel 6 – Condiţii pentru înlocuirea certificatului după revocare

3.4 Cererea de revocare

Înainte de revocarea unui certificat, DigiSign verifică faptul că revocarea a fost solicitată de către posesorul certificatului, entitatea care a aprobat cererea de certificat. Procedurile agreate pentru autentificarea cererilor de revocare ale utilizatorului includ:

- Trimiterea de către utilizator a parolei de verificare şi revocarea automată a certificatului, dacă aceasta se potriveşte cu parola de verificare oficială;
- Primirea unui mesaj cu explicaţii din partea utilizatorului care solicită revocarea şi care conţine de asemenea o semnătură digitală, care poate fi verificată, în legătură cu certificatul care urmează să fie revocat;
- Comunicarea cu utilizatorul, care furnizează asigurări cu privire la faptul că persoană care solicită revocarea este chiar utilizatorul. În funcţie de circumstanţe, această comunicare se realizează prin: telefon, fax, e-mail, poştă sau servicii de curierat.

Administratorii DigiSign au dreptul să solicite revocarea certificatelor utilizatorului final.

Cererile din partea DigiSign de a revoca un certificat AC sunt autentificate de către un quorum de decizie, pentru a asigura că revocarea a fost de fapt solicitată de către AC.

4. Cerinţe operaţionale

4.1 Cererea pentru certificat

4.1.1 Cererea pentru certificat depusa pentru certificatele utilizatorului final

Pentru certificate DigiSign, toţi solicitanţii de certificate vor urma procesul de înscriere, care constă din:

- Completarea unei cereri pentru certificat şi furnizarea informaţiilor cerute,
- Generarea sau crearea condiţiilor pentru generarea unei perechi de chei, în concordanţă cu punctul § 6.1,
- Demonstrarea către DigiSign în continuarea punctului § 3.1.7 că solicitantul certificatului deţine cheia privată corespunzătoare cheii publice transmisă către DigiSign,
- Manifestarea acordului serviciului aferent.

Cererile pentru certificat sunt trimise la DigiSign pentru procesare, aprobare sau respingere. Entitatea care procesează cererea pentru certificat, conform punctului § 4.2 poate fi reprezentată de două entităţi, după cum se arată în tabelul următor.

Clasa certificatului/Categoria	*Entitatea care procesează cererile pentru certificate*	*Entitatea care eliberează certificate*
Certificate calificate DigiSign	DigiSign S.A.	DigiSign S.A.
CA, Infrastructura	DigiSign S.A.	DigiSign S.A.

Tabel 7 – Entităţi care primesc cererile pentru certificate

4.1.2 Cererile de certificate pentru AC, AI

4.1.2.1 Certificate AC

Pentru AC-urile DigiSign, cererile de certificate sunt create şi aprobate de către personalul autorizat, printr-un proces de control ce necesită participarea mai multor persoane de încredere.

4.1.2.2 Certificate AI

DigiSign S.A. operează task-uri administrative care emit certificate pentru AI-uri şi sisteme AI, incluzând:

- Personalul DigiSign (administratorii DigiSign) care procesează cererile pentru certificate în numele DigiSign, în cadrul DigiSign
- Serverele de administrare automată care procesează cererile pentru certificate pentru DigiSign, unde s-a stabilit un proces de autentificare şi administrare automată.

Pentru toate aceste AI, ca abonaţi la AC-ul administrativ aferent, se aplică cerinţele pentru certificatele administrator clasa 3, specificate în CPP la punctul § 4.1.1.

4.2 Emiterea certificatului

4.2.1 Emiterea certificatelor pentru utilizatorul final

După ce un solicitant de certificat trimite cererea, DigiSign, (vezi punctul § 4.1.1) încearcă să confirme informaţiile din aceasta cerere (altele decât informaţiile neverificate despre utilizator), conform CPP §§ 3.1.8.1, 3.1.9. După îndeplinirea cu succes a tuturor procedurilor de autentificare solicitate la punctul § 3.1, administratorul DigiSign aprobă cererea pentru certificat. Dacă procesul de autentificare nu are succes, DigiSign respinge cererea pentru certificat.

Un certificat este procesat şi eliberat în urma aprobării unei cereri sau pe baza primirii unei cereri a AI de a elibera certificatul. Când DigiSign aprobă o cerere pentru certificat şi comunică acceptul către utilizator, DigiSign procesează un certificat şi îl eliberează solicitantului de certificat. Procedurile acestei secţiuni se folosesc , de asemenea, şi pentru emiterea de certificate în cazul unei cereri pentru a înlocui (a reînnoi) un certificat.

4.2.2 Eliberarea de certificate pentru AC, AI şi infrastructură

DigiSign S.A. eliberează certificatele necesare pentru ca DigiSign să îndeplinească funcţii de AC sau AI.

4.3 Acceptarea certificatului

După generarea certificatului, DigiSign S.A. înştiinţează abonaţii că certificatele lor sunt disponibile şi le transmit procedurile de intrare în posesie.

După eliberare, certificatele sunt disponibile pentru utilizatorii finali. Certificatul poate fi trimis solicitantului in urmatoarele modalitati

- Prin posta, cu confirmare la primire(pentru certificatele calificate)
- Personal (pentru certificatele calificate)

Numai pentru certificate simple

- DigiSign poate trimite utilizatorului un cod PIN pe care acesta îl introduce în pagina de web de înscriere pentru a obţine certificatul. Descărcarea unui certificat sau instalarea sa dintr-un mesaj care îl are ataşat, reprezintă acceptarea certificatului de către utilizator.

4.3.1 Revocarea certificatului

4.3.1.1 Circumstanţe pentru revocarea certificatelor utilizatorului final

Un certificat al utilizatorului final este revocat dacă:

- DigiSign sau un utilizator are motive puternice să creadă că a fost compromisă cheia privată a utilizatorului,
- DigiSign S.A. are motive să creadă că utilizatorul a încălcat o obligaţie materială, de reprezentare sau de garanţie, conform acordului dintre părţi,
- Acordul dintre părţi s-a încheiat,
- DigiSign S.A. are motive să considere că certificatul nu a fost eliberat în conformitate cu procedurile solicitate de codul de practici şi proceduri, certificatul a fost eliberat unei alte persoane decât cea numită drept subiect al certificatului sau certificatul a fost eliberat fără autorizarea persoanei numite drept subiect al certificatului,
- DigiSign S.A. are motive să considere că anumite informaţii din cererea pentru certificat sunt false;
- DigiSign S.A. stabileşte că nu a fost îndeplinită sau a fost amânată o condiţie esenţială pentru eliberarea certificatului;
- Informaţiile din certificat, altele decât informaţiile neverificate despre utilizator, sunt incorecte sau s-au schimbat;
- Utilizatorul solicită revocarea certificatului în concordanţă cu punctul § 3.4.

DigiSign poate revoca de asemenea un certificat de administrator dacă autoritatea administratorului de a acţiona ca administrator s-a încheiat sau s-a terminat din alte motive.

Acordul dintre părţi al DigiSign solicită utilizatorilor finali sa anunţe imediat DigiSign, în cazul în care se bănuieşte sau chiar a avut loc compromiterea cheilor private.

DigiSign se obliga sa revoce certificatul utilizatorului final in termen de 24 de ore de la indeplinirea conditiilor mentionate mai sus.

4.3.1.2 Circumstanţe pentru revocarea certificatelor de AC sau AI

DigiSign S.A. va revoca certificatele de AC sau AI, în cazul în care:

- DigiSign descoperă sau are motive să considere că a fost compromisă cheia privată a AC sau AI DigiSign;
- DigiSign descoperă sau are motive să considere că certificatul nu a fost eliberat în conformitate cu procedurile solicitate de codul de practici şi proceduri, certificatul a fost eliberat unei alte persoane decât cea numită drept subiect al certificatului sau certificatul a fost eliberat fără autorizarea persoanei numite drept subiect al certificatului;
- DigiSign S.A. stabileşte că nu a fost îndeplinită sau a fost amânată o condiție esențială pentru eliberarea certificatului;
- DigiSign S.A. solicită revocarea certificatului.

4.3.2 Solicitarea revocării

4.3.2.1 Următoarele entități pot solicita revocarea unui certificat al utilizatorului final:

- DigiSign S.A., care a aprobat cererea utilizatorului pentru certificat, poate solicita revocarea oricărui certificat al unui utilizator final sau al unui administrator.
- Abonații individuali pot solicita revocarea propriilor certificate.
- Un reprezentant autorizat al DigiSign, care a primit un certificat de administrator, este îndreptățit să solicite revocarea unui certificat de administrator.

4.3.2.2 Următoarele entități pot solicita revocarea unui certificat AC, AI sau de infrastructură:

- Numai DigiSign este îndreptățită să solicite sau să inițieze revocarea certificatului emis propriilor componente AC sau AI.

4.3.3 Procedura pentru solicitarea revocării

4.3.3.1 Procedura pentru solicitarea revocării unui certificat al utilizatorului final

Un utilizator final care solicită revocarea trebuie să comunice aceasta cerere la DigiSign S.A. Comunicarea unei astfel de revocări se va face în concordanță cu punctul § 3.4.

4.3.3.2 Procedura pentru solicitarea revocării unui certificat AC sau AI

Consiliul de administratie impreuna cu membrii qvorumului de acces (m of n) pot decide revocarea cheilor unui certificat AC sau AI al Digisign S.A si pot initia procedura de revocare a acestora.

4.3.4 Perioada de grație pentru solicitarea revocării

Cererile de revocare trebuie trimise cât mai prompt într-o perioadă de timp rezonabilă.

4.3.5 Circumstanțe pentru suspendare

DigiSign nu oferă, în general, servicii de suspendare a certificatelor pentru utilizatorii finali.

4.3.6 Frecvența publicării listei de revocare a certificatelor

DigiSign publică liste de revocare a certificatelor, arătând starea de revocare a certificatelor şi oferă servicii de control a situației. Listele de revocare a certificatelor pentru AC-urile care emit certificate de AC sunt publicate trimestrial şi, de asemenea, ori de câte ori este revocat un certificat AC. Certificatele expirate sunt retrase din listele de revocare a certificatelor la treizeci (30) de zile după expirare.

4.3.7 Cerințe pentru verificarea listei de revocare a certificatelor

O metodă prin care părțile, având o relație de încredere pot verifica starea certificatului este consultarea celei mai recente liste de revocare a certificatelor, publicată de către AC-ul care a emis certificatul pe care doresc să se bazeze acestea.

Pentru DigiSign S.A., listele de revocare a certificatelor sunt expediate la **Digisign CRL** sau in registrul DigiSign.

Un tabel de referință privind starea certificatelor este publicat în registru pentru a ajuta părțile, având o relație de încredere să determine starea de revocare a certificatelor pentru AC-ul aferent.

4.3.8 Revocare on-line / disponibilitate pentru verificarea statutului

Pe lângă publicarea listelor de revocare a certificatelor, DigiSign, furnizează informaţii despre statutul certificatului, prin interogarea unor baze de date din registrul propriu.

4.3.9 Cerinţe pentru verificarea revocării on-line

Dacă o parte nu verifică statutul certificatului pe care doreşte să se bazeze, consultând cea mai recentă listă de revocare a certificatelor, trebuie să facă acest lucru folosind una dintre metodele specificate la punctul § 4.4.11.

4.3.10 Cerinţe speciale privind compromiterea cheii

DigiSign depune eforturi pentru a înştiinţa părţile dacă descoperă, are motive să considere sau chiar a fost compromisă cheia privată a DigiSign AC.

4.4 Proceduri de verificare a securităţii

4.4.1 Tipuri de evenimente înregistrate

DigiSign S.A. monitorizează manual sau automat următoarele evenimente semnificative:

- Evenimente legate de administrarea cheii AC, incluzând:
  - Generarea cheii, backup, stocare, recuperare, arhivare şi distrugere
  - Evenimente legate de dispozitivul criptografic pentru administrarea continuă.
- Evenimente legate de administrarea certificatului AC şi a utilizatorului, incluzând:
  - Cererile pentru certificate, înnoirea, înlocuirea şi revocarea
  - Procesarea reuşită sau nereuşită a cererilor
  - Generarea şi emiterea de certificate şi liste de revocare a certificatelor.
- Evenimente legate de securitate, incluzând:
  - Încercări reuşite sau nereuşite de acces la sistemul infrastructurii cheii publice
  - Acţiuni ale infrastructurii cheii publice şi ale sistemului de securitate pe care le execută personalul DigiSign
  - Dosare sau înregistrări sensibile de securitate, citite, scrise sau şterse
  - Schimbări în profilul securităţii
  - Căderi ale sistemului, ratări ale hardware-ului şi altele

- Activitate de firewall şi router
- Intrarea/ieşirea din locaţia AC, destinată vizitatorilor.

Intrările în fişierul de log cuprind următoarele elemente:

- Data şi ora intrării
- Numărul serial sau de ordine al intrării, pentru intrările automate
- Identitatea entităţii care realizează intrarea
- Tipul de intrare.

AI-urile DigiSign şi administratorii DigiSign monitorizează informaţiile cererii de certificat, incluzând:

- Tipul de document(e) de identificare prezentate de către solicitantul certificatului;
- Dosar al datelor unice de identificare, numere sau o combinaţie (de ex. numărul carnetului de conducere al solicitantului) a documentelor de identificare, dacă este posibil;
- Locaţia stocării copiilor după aplicaţii şi după documentele de identificare;
- Identitatea entităţii care acceptă aplicaţia;
- Metoda folosită pentru a valida documentele de identificare, dacă există;
- Numele AC-ului care primeşte sau al AI-ului care trimite, dacă este posibil.

4.4.2 Frecvenţa procesării de loguri

Log-urile de verificare sunt examinate cel puţin o data pe săptămână pentru evenimente semnificative de securitate şi operaţionale. În plus, DigiSign S.A trece în revista log-urile sale de verificare pentru activităţi suspecte sau neobişnuite, ca răspuns la alertările generate şi bazate pe iregularitati şi incidente în cadrul sistemului AC.

Procesarea log-ului de verificare constă din revizuirea log-urilor de verificare şi a documentaţiei pentru toate evenimentele semnificative într-un sumar al log-ului de verificare. Revizuirea log-ului de verificare include verificarea faptului ca log-ul nu a fost falsificat, o scurtă inspectare a tuturor intrărilor în fişierul de log şi o investigare mai profundă a oricăror alertări sau iregularitati din log-uri. Acţiunile care se întreprind, bazate pe revizuirile log-ului de verificare, trebuie de asemenea să fie susţinute cu documente.

4.4.3 Perioada de păstrare pentru log-ul de verificare

Log-urile de verificare sunt reținute pe site cel puțin două (2) luni după procesare și după aceea sunt arhivate, în concordanță cu punctul § 4.6.2.

4.4.4 Protecția log-ului de verificare

Fișierele log-ului de verificare electronică și manuală sunt protejate împotriva examinării neautorizate, modificării, ștergerii sau altor tipuri de falsificări prin folosirea controalelor de acces fizic și logic.

4.4.5 Proceduri de salvare a log-ului de verificare

Salvările incrementale ale log-urilor de verificare sunt create zilnic, iar copiile complete de siguranță sunt realizate săptămânal.

4.4.6 Sistemul de adunare a verificării

Datele verificării automate sunt generate și păstrate la nivel de aplicație, rețea și nivel de sistem operațional. Datele verificării, generate manual sunt păstrate de către personalul DigiSign S.A.

4.4.7 Înștiințarea subiectului care produce evenimentul

Când un eveniment este monitorizat de către sistemul de cumulare a verificării, nu este obligatorie notificarea persoanelor fizice, organizației, dispozitivului sau aplicației care a condus la eveniment.

4.4.8 Evaluarea vulnerabilității

Evenimentele din procesul de verificare sunt monitorizate, parțial, pentru a monitoriza vulnerabilitățile sistemului. Evaluările vulnerabilității securității logice (EVSL) sunt realizate, trecute în revistă și revizuite în urma unei examinări a acestor evenimente monitorizate. EVSL-urile se bazează pe date de monitorizare automată în timp real și sunt realizate zilnic, lunar și anual, în concordanță cu cerințele ghidului privind securitatea informatiei si securitatea PKI. O evaluare anuală servește ca prim element de intrare în verificarea anuală a conformității.

4.5 Dosarele de arhivă

4.5.1 Tipuri de evenimente înregistrate

Pe lângă log-urile de verificare specificate la punctul § 4.5, DigiSign păstrează, atunci când i se cere, documentația pentru:

- Acționarea DigiSign, în conformitate cu codul de practici şi proceduri şi alte obligații din acordurile cu abonații,
- Acțiuni şi informații esențiale pentru fiecare cerere de certificat şi pentru emiterea, eliberarea, folosirea, revocarea, expirarea şi înlocuirea tuturor certificatelor care se emit .

Înregistrările DigiSign despre evenimentele legate de certificat includ:

- Identitatea utilizatorului numit în fiecare certificat,
- Identitatea persoanei care solicită revocarea certificatului,
- Alte fapte reprezentate în certificat;
- Anumite fapte esențiale previzibile, legate de emiterea certificatului inclusiv, dar nu limitându-se la atât, informații relevante pentru încheierea cu succes a verificării conformității, conform punctului § 2.7.

Înregistrările pot fi menținute electronic sau pe o copie pe hard, cu condiția ca acestea să fie indexate, stocate, păstrate şi reproduse în mod corespunzător şi complet.

4.5.2 Perioada de păstrare în arhivă

Înregistrările legate de certificatele calificate DigiSign sunt păstrate zece (10) de ani de la data expirării sau revocării certificatului.

Dacă este necesar, DigiSign S.A. poate implementa perioade mai lungi de păstrare, pentru a se conforma legilor în vigoare.

4.5.3 Protecția arhivei

DigiSign S.A. îşi protejează dosarele arhivate, alcătuite conform punctului § 4.6.1, astfel încât numai persoanele de încredere autorizate să aibă acces la datele arhivate. Datele arhivate electronic sunt protejate împotriva examinării neautorizate, modificării, ştergerii sau altui tip de falsificare, prin implementarea controalelor corespunzătoare de acces fizic şi logic. Mediile care dețin datele arhivate şi aplicațiile

solicitate pentru a procesa datele arhivate sunt menţinute pentru a asigura faptul că datele arhivate pot fi accesate în perioada stabilită la punctul § 4.6.2.

4.5.4 Proceduri de salvare a arhivei

DigiSign S.A realizează zilnic arhive electronice care conţin informaţii despre certificatele sale emise şi execută saptamanal copii de siguranţă completă. Copii ale înregistrărilor păstrate pe hârtii, conform punctului § 4.6.1, sunt menţinute într-o locaţie de recuperare din afara site-ului, în concordanţă cu punctul § 4.8.

4.5.5 Cerinţe pentru ştampila de timp aplicată înregistrărilor

Certificatele, listele de revocare a certificatelor şi alte intrări în baze de date de revocare conţin informaţii referitoare la oră şi dată. Trebuie notat faptul că astfel de informaţii despre oră nu se bazează pe algoritm criptografic, nici nu beneficiaza de serviciul time-stamping.

4.6 Schimbarea cheii

Perechile de chei ale AC-ului DigiSign sunt retrase din folosinţă la sfârşitul perioadei maxime de valabilitate, după cum se defineşte la punctul § 6.3.2. Certificatele AC-ului DigiSign pot fi reînnoite atât timp cât perioada cumulativă de valabilitate certificata a perechii de chei a AC nu depăşeşte perioada maximă de valabilitate a perechii de chei a AC. Dacă este necesar, vor fi generate noi perechi de chei pentru AC, de exemplu pentru a înlocui perechi de chei ale AC care au fost retrase, pentru a le suplimenta pe cele existente, active şi pentru a susţine noi servicii, în concordanţă cu punctul § 6.1.

Înainte de expirarea certificatului de AC pentru un AC superior, sunt iniţiate procedurile de schimbare a cheii, pentru a facilita o trecere lină a entităţilor în ierarhia AC-ului superior de la vechea pereche de chei de AC superior la o nouă pereche de chei de AC. Procesul de schimbare a cheii de AC a DigiSign solicită ca:

- Un AC superior să înceteze să emită noi certificate subordonate AC, nu mai târziu de 60 de zile înainte de data ("data de încetare a emiterii") la care timpul rămas din valabilitatea perechii de chei de CA superior este egal cu perioada de valabilitate a certificatului, aprobată pentru tipuri precise de certificate eliberate de AC-uri subordonate în ierarhia AC-ului superior.
- După validarea cu succes a cererilor pentru certificat de AC subordonat (sau utilizator final) primite după "data de încetare a emiterii", certificatele vor fi semnate cu o noua pereche de chei de AC.

- AC-ul superior să continue să elibereze liste de revocare a certificatelor semnate cu cheia privată originală a AC-ului superior, până la data de expirare a ultimului certificat emis prin folosirea perechii originale de chei.

4.7 Compromiterea cheii

Pe baza suspectării sau a certitudinii privind compromiterea unui AC DigiSign, echipa de răspuns la incidentul compromiterii (ERIC) iniţiază procedurile de răspuns în cazul compromiterii cheii. Această echipa, care include personal din securitate, operaţii criptografice de afaceri, servicii de producţie şi alţi reprezentanţi ai managementului, evaluează situaţia, dezvoltă un plan de acţiune şi implementează acest plan, având aprobarea managementului executiv al DigiSign S.A.

Dacă este solicitată revocarea certificatului de AC, se întreprind următoarele proceduri:

- Este comunicată părţilor de încredere situaţia certificatului revocat, prin registrul DigiSign S.A.,
- AC-ul va genera o nouă pereche de chei, excepţie făcând cazul în care AC-ul este limitat.

4.8 Încheierea AC

În cazul în care AC-ul DigiSign îşi încetează activitatea, se obligă să înştiinţeze abonaţii şi alte entităţi afectate cu privire la încetarea activităţii, cu respectarea art. 24 din Legea nr. 455/2001 privind semnătura electronică. În această situaţie, DigiSign S.A. se obligă să elaboreze un plan de acţiune care să cuprindă următoarele:

- Dispoziţia de notificare a părţilor afectate de încheiere, precum abonaţii, informându-i cu privire la situaţia AC-ului,
- Administrarea costurilor pentru această notificare,
- Revocarea certificatului eliberat de DigiSign pentru AC,
- Păstrarea arhivelor şi dosarelor AC-ului pentru perioadele de timp stabilite de Legea nr. 455/2001 privind semnătura electronică,
- Continuarea serviciilor de suport pentru utilizator şi client,
- Continuarea serviciilor de revocare, precum emiterea de liste de revocare a certificatelor sau menţinerea serviciilor de verificare online a situaţiei,
- Revocarea certificatelor neexpirate şi nerevocate ale abonaţilor utilizatori finali şi ale AC-urilor subordonate, dacă este necesar,

- Plata compensației (dacă este necesar) pentru abonații ale căror certificate neexpirate şi nerevocate sunt revocate din cauza planului de încheiere sau aprovizionarea sau, alternativ, eliberarea de certificate de înlocuire de către un AC care va urma,
- Consemnarea cheii private a AC-ului şi a cardurilor hardware care conțin o astfel de cheie privată,
- Prevederile necesare pentru trecerea serviciilor AC-ului la AC-ul care va urma.

5. Controale de securitate fizică, procedurală şi de personal

DigiSign a implementat politica de securitate DigiSign, care susține cerințele de securitate prezentate în acest cod de practici şi proceduri.

5.1 Controale fizice

5.1.1 Amplasare şi construcție

Operațiile de AC ale DigiSign sunt dirijate din cadrul locației str Virgil Madgearu 2-6, care satisfac cerințele securității şi cerințele de verificare. Toate operațiile de AC şi AI ale DigiSign sunt dirijate dintr-un mediu protejat desemnat pentru a împiedica, a preveni şi a detecta penetrarea ascunsă sau fățişă.

Locațiile primare ale Digisign au până la cinci nivele de securitate, cu:

- Operațiile de validare ale AI întreprinse în cadrul nivelului 3;
- Funcțiile AC întreprinse în cadrul nivelului 4;
- Servere sensibile, incluzând server-ul DIGISIGN PUBLIC CA, localizat la nivelul 4;
- Module criptografice online de AC stocate la nivelul 5;
- Module criptografice offline de AC, stocate la nivelul 5.

Locațiile securizate ale DigiSign îndeplinesc cerințele ghidului de securitate al societății.

5.1.2 Acces fizic

Sistemele AC ale DigiSign sunt protejate pe nivele de securitate fizică, cu solicitarea accesului la un nivel inferior înainte de a câştiga acces la unul superior. În plus, sistemul de securitate fizică include şi nivele suplimentare pentru securitatea administrării cheilor criptografice.

Accesul la primul nivel necesită folosirea unui card de proximitate ca ecuson pentru angajaţi(sau amprenta digitala). Accesul fizic la nivelul unu este logat automat. Nivelul doi de securitate asigura controlul accesului tuturor persoanelor care pătrund in aria AC prin utilizarea cardului de proximitate. Personalul ne-escortat, incluzând angajaţii care nu beneficiază de acces liber, nu au voie să intre într-o arie securizată la acest nivel. Accesul fizic la acest nivel este logat automat.

Nivelul trei al centrului de date întăreşte controlul accesului individual. Persoanele fizice care se bucură de acces ne-escortat la acest nivel trebuie să satisfacă politica angajatului de încredere. Şi acest acces fizic este logat automat.

Cheile criptografice ale AC DigiSign SA sunt păstrate si protejate la sediul din Virgil Madgearu 2-6. Sistemele AC ale DigiSign sunt protejate de patru nivele de securitate fizică, cu solicitarea accesului la un nivel inferior înainte de a câştiga acces la unul superior. În plus, sistemul de securitate fizică include şi nivele suplimentare pentru securitatea administrării cheilor criptografice.

Mecanismul de control acces
Accesul la acest nivel necesită utilizarea unui card de proximitate. Accesul la acest nivel este monitorizat şi înregistrat automat.
Nivelul doi impune controlul accesul individual pentru toate persoanele care pătrund în aria AC, facilitate care

	necesită utilizarea cardului de proximitate. Accesul fizic la nivelul doi este monitorizat automat.
	Nivelul trei impune accesul individual utilizând a doi factori de autentificare, inclusiv cel biometric. Personalului ne-escortat, inclusiv angajaţilor neverificaţi şi vizitatorilor nu li se permite accesul fizic la acest nivel. Şi accesul la acest nivel este monitorizat.
	Nivelul patru al centrului de date impune controlul accesului individual iar camera pentru ceremonia cheii impune controlul dual, fiecare prin utilizarea unui factor dublu de autentificare, inclusiv unul biometric. Aprobarea accesului individual neescortat la nivelul patru trebuie să satisfacă cerinţele politicii angajaţilor de încredere. Accesul la acest nivel este monitorizat automat.
	CSU-urile online sunt protejate prin folosirea dulapurilor încuiate. Accesul la CSU-uri şi la materialul important este restricţionat, în concordanţă cu cerinţele DigiSign de separare a îndatoririlor. Deschiderea şi închiderea dulapurilor sau containerelor de la aceste nivele este log-ata în scopul verificării. Accesul fizic restricţionat din ce în ce mai mult ajută controlul accesului la fiecare nivel.

5.1.3 Energie şi aer condiţionat

Locaţiile securizate ale DigiSign sunt echipate cu salvarea de siguranţă fundamentală:

- Sisteme energetice pentru a asigura acces continuu şi neîntrerupt la energia electrica
- Sisteme de încălzire/ventilaţie/aer condiţionat pentru a controla temperatura şi umiditatea relativă.

5.1.4 Expunerile la apă

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

5.1.5 Prevenirea şi protecţia împotriva focului

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

5.1.6 Mediul de stocare

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

5.1.7 Dispunerea lucrurilor nefolositoare

Documentele şi materialele sensibile sunt rupte înainte de a fi aruncate. Mijloacele folosite pentru a strânge sau a transmite informaţiile sensibile nu mai pot fi citite, înainte de a fi aruncate. Înainte de a fi aruncate, dispozitivele criptografice sunt distruse fizic sau minimizate, în concordanţă cu îndrumările anterioare ale producătorului. Alte lucruri nefolositoare sunt aruncate, ţinând cont de cerinţele DigiSign.

5.1.8 Salvarea off-site

DigiSign S.A. întreprinde salvările de rutină ale datelor importante de sistem, ale datelor despre log-urile de verificare şi ale altor informaţii sensibile.

5.2 Controale procedurale

5.2.1 Funcţii de încredere

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

- Validarea informaţiilor din cererile pentru certificate;

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

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

- Personalul de la serviciu clienți,
- Personalul care se ocupa de operațiile criptografice ale activității,
- Personalul de securitate,
- Personalul de la sistemul de administrare,
- Personalul de la departamentul tehnic,
- Directorii care se ocupă cu administrarea loialității de infrastructură.

DigiSign S.A. consideră categoriile de personal identificate mai sus, în aceasta secțiune, drept persoane de încredere ce au o poziție de încredere. Persoanele care doresc sa devină persoane de încredere prin obținerea unei poziții de încredere trebuie să îndeplinească cerințele de selecție prezentate la punctul § 5.3.

5.2.2 Numărul de persoane necesare pentru fiecare sarcina

DigiSign S.A. menține o politică şi proceduri de control riguroase pentru a asigura separarea responsabilităților. Cele mai sensibile sarcini, precum accesul şi managementul hardware-ului criptografic al AC (elementele de semnare criptografica sau CSU) şi materialul asociat, necesită mai multe persoane de încredere.

Aceste proceduri de control intern sunt desemnate pentru a asigura că cel puțin doi dintre membrii de încredere trebuie să aibă acces fizic sau logic la dispozitiv. Accesul la hardware-ul criptografic al AC este strict intensificat prin intermediul mai multor persoane de încredere de-a lungul ciclului său de funcționare, de la primire şi recepție până la distrugerea finală logică şi/sau fizică. După ce un modul este activat cu chei operaționale, sunt invocate controalele de acces pentru a menține controlul separat asupra accesului fizic şi logic la dispozitiv. Persoanele care au acces fizic la module nu dețin "părțile secrete" şi viceversa. Cerințele pentru datele de activare a cheii private a AC şi părțile secrete sunt specificate la punctul § 6.2.7.

Alte operaţii precum validarea şi emiterea de certificate clasa 3 necesită participarea a cel puţin 2 persoane de încredere.

5.2.3 Identificarea şi autentificarea pentru fiecare funcţie

Pentru tot personalul care doreşte să se numere printre persoanele de încredere, verificarea identităţii se realizează prin prezenţa sa fizică în faţa persoanelor de încredere ale DigiSign S.A. de la departamentul Resurse Umane sau având funcţii în securitate şi se realizează o verificare a actelor de identificare. Identitatea este confirmată apoi prin procedurile de verificare de fond, prevăzute la punctul § 5.3.1.

DigiSign S.A. asigură că, personalul a dobândit statutul de încredere şi că a primit aprobarea departamentală, înainte ca acestor persoane să li se:

- Emită dispozitivele de acces şi accesul la locaţiile solicitate;
- Emită legitimaţii electronice pentru a avea acces şi pentru a îndeplini funcţii precise la DigiSign sau la alte sisteme IT.

5.3 Controale de personal

5.3.1 Cerinţe privind trecutul, calificările, experienţa şi acceptarea

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

5.3.2 Proceduri de verificare a informaţiilor cu privire la personal

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

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

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

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

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

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

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

5.3.3 Cerinţe de pregătire

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

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

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

5.3.4 Cerinţele şi frecvenţa cursurilor de perfecţionare

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

5.3.5 Sancţiuni pentru acţiuni neautorizate

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

5.3.6 Cerinţe pentru contractarea personalului

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

Contractanţii şi consultanţii independenţi care nu au desăvârşit procedurile de verificare a trecutului specificate la punctul § 5.3.2 pot accesa locaţiile securizate ale DigiSign numai dacă sunt escortaţi şi supravegheaţi direct de persoane de încredere.

5.3.7 Documentaţie furnizată personalului

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

6. Controale de securitate tehnica

6.1 Generarea şi instalarea perechii de chei

6.1.1 Generarea perechii de chei

Generarea perechii de chei a AC este realizată de mai multe persoane de încredere, selectate şi pregătite, care folosesc sisteme de încredere şi procese care deţin securitatea şi puterea criptografică necesară cheilor generate. Modulele criptografice folosite pentru generarea cheii îndeplinesc cerinţele FIPS 140-2 nivel 3.

Toate perechile de chei ale AC sunt generate în cadrul unei ceremonii prestabilite de generare a cheii, în concordanţă cu cerinţele ghidului de ceremonie a cheii, ale ghidului pentru utilizatorii instrumentelor de management ale cheii AC şi ale ghidului de securitate şi al cerinţelor de verificare. Sunt înregistrate toate activităţile întreprinse în fiecare ceremonie de generare a cheii, sunt datate şi semnate de către toate persoanele implicate. Aceste înregistrări sunt păstrate, în scopul verificării şi urmăririi, pe o perioada de timp considerată corespunzătoare de către administraţia DigiSign.

Generarea perechilor de chei ale AI este realizată în general de către AI folosind un modul criptografic certificat FIPS 140-2 nivel 3.

Generarea perechii de chei pentru utilizatorul final este realizată, în general, de către utilizator. Pentru certificatele calificate ale DigiSign, utilizatorul foloseşte un modul criptografic certificat FIPS 140-2 nivel 2.

DigiSign nu duplica si nu stocheaza in nici un fel cheia privata a utilizatorului final.

6.1.2 Livrarea către entitate a cheii private

Perechile de chei ale utilizatorului final sunt generate, de obicei, de către utilizatorul final. De aceea, în aceste cazuri, livrarea cheii private către utilizator nu se poate realiza.

Când perechile de chei ale AI sau ale utilizatorului final sunt pregenerate de DigiSign) pe carduri hardware sau pe smartcard, astfel de dispozitive sunt distribuite către AI sau către utilizatorul final, folosind un serviciu comercial de livrare şi un pachet care să

demonstreze integritatea conținutului. Datele necesare pentru activarea dispozitivului sunt comunicate către AI sau către utilizatorul final, folosind un proces în afara benzii. Distribuirea acestor tipuri de dispozitive este urmărită de DigiSign.

6.1.3 Livrarea cheii publice către emitentul de certificate

Perechile de chei ale utilizatorului final sunt generate la sediul DigiSign, sub supravegherea personalului instruit.

6.1.4 Livrarea cheii publice de autoritatea de certificare către utilizatori

DigiSign S.A. furnizează, în general, întreg lanțul de certificate (inclusiv AC-ul care emite şi orice alt AC din lanț) pentru utilizatorul final pe emisiunea de certificate. Certificatele AC DigiSign pot fi, de asemenea, descărcate de pe site-ul propriu, la Lantul de Incredere

6.1.5 Mărimile cheii

Perechile de chei de AC ale DigiSign sunt de cel puțin 2048 bit RSA, DigiSign S.A. obliga utilizatorii finali să genereze perechi de chei de cel putin 1024 bit RSA.

6.1.6 Generarea cheii de hardware/software

DigiSign S.A. generează perechile de chei de AC pentru DigiSign S.A. in module criptografice de hardware corespunzătoare, în conformitate cu punctul § 6.2.1. Perechile de chei ale utilizatorului final trebuie să fie generate, de asemenea, pe hardware.

6.1.7 Scopurile utilizării cheii

Pentru certificatele X.509 versiunea 3, DigiSign completează, în general, extensia "KeyUsage" (utilizarea cheii) a certificatelor, în concordanță cu RFC 2459: Internet X.509 - Infrastructura cheii publice a certificatelor şi profilul LCR, ianuarie 1999. Extensia "KeyUsage" în certificatele X.509 versiunea 3 este completată, în concordanță cu tabelul 9 de mai jos, cu următoarele excepții:

		CA-uri	*Carduri de administrare automata*
Criticalitate		FALS	FALS
0	Semnătura	-	Set

		CA-uri	*Carduri de administrare automata*
	digitală		
1	Non-repudiere	-	-
2	Cifrarea Cheii	-	Set
3	Cifrarea Datelor	-	-
4	keyAgreement	-	-
5	keyCertSign	Set	-
6	CRLSign	Set	-
7	Criptare	-	-
8	Decriptare	-	-

Tabel 9 – Setări pentru extensia KeyUsage

6.2 Protecţia cheii private

DigiSign S.A. a implementat o combinaţie de controale fizice, logice şi procedurale pentru a asigura securitatea cheilor private ale DigiSign. Controalele accesului fizic sunt descrise la punctul § 5.1.2. Utilizatorii trebuie să-şi ia măsurile de precauţie necesare pentru a preveni pierderea, dezvăluirea, modificarea sau folosirea neautorizată a cheilor private.

6.2.1 Standarde pentru modulele criptografice

Pentru generarea perechii de chei de root AC DigiSign şi stocarea cheii private de AC, DigiSign S.A. foloseşte module de hardware criptografic, ce sunt certificate sau satisfac cerinţele FIPS 140-2 nivel 3. .

6.2.2 Controlul cheii private realizat de mai multe persoane

DigiSign S.A. a implementat mecanisme tehnice şi procedurale care solicită participarea mai multor persoane de încredere la întreprinderea operaţiilor criptografice sensibile de către AC. DigiSign S.A. foloseşte "împărţirea secretă" pentru a partaja datele de activare necesare, pentru a folosi cheia privata a AC, în părţi separate numite "parţi secrete" şi care sunt deţinute de către "posesori" pregătiţi şi de încredere. Este necesar un număr de părţi secrete (n) din numărul total de părţi secrete create şi distribuite pentru un anumit modul (m) criptografic de hardware pentru a activa o cheie privată de AC, stocată pe modul.

6.2.3 Păstrarea în custodie a cheii private

DigiSign nu lasă în custodie unui terț cheile private ale AI sau ale utilizatorului final, în scopul accesului, prin aplicarea legii.

6.2.4 Salvarea cheii private

DigiSign stochează copii ale cheilor private ale AI conform cu procedura de restaurare in caz de dezastru, folosind dispozitive certificate FIPS 140-2, level3 si CC EAL 4+ . Pentru salvarea cheilor private ale utilizatorului final, a se vedea punctul § 6.2.3.

6.2.5 Arhivarea cheii private

Când se încheie perioada de valabilitate a perechilor de chei ale AC DigiSign, aceste perechi de chei ale AC vor fi arhivate pentru o perioada de cel puţin 5 ani. Perechile de chei private ale AC vor fi stocate în siguranță de către DigiSign S.A., folosind module criptografice hardware care satisfac cerințele punctului § 6.2.1. Controalele procedurale împiedică faptul ca perechile arhivate de chei ale AC să fie returnate şi folosite în scop de producție. La sfârşitul perioadei de arhivare, cheile private arhivate vor fi distruse în siguranța, în concordanță cu punctul § 6.2.9.

DigiSign nu arhivează copii ale cheilor private ale AI şi ale utilizatorului final.

6.2.6 Intrarea cheii private în modulul criptografic

DigiSign S.A generează perechile de chei de AC pe modulele de hardware criptografic în care vor fi folosite cheile.

6.2.7 Metoda de activare a cheii private

Toţi abonaţii DigiSign S.A. trebuie să protejeze datele de activare a cheilor lor private împotriva pierderii, furtului, modificării, dezvăluirii neautorizate sau folosirii neautorizate.

6.2.7.1 Cheile private ale utilizatorului final

Aceasta secţiune aplică standardele europene pentru protejarea datelor de activare a cheilor private ale utilizatorilor finali. Mai mult, utilizatorii trebuie sa folosească dispozitive de creare a semnăturii digitale securizate, precum smartcard-uri, eToken pentru stocarea cheilor private. Se încurajează folosirea a două mecanisme de autentificare (card şi parola, dispozitiv biometric şi card sau dispozitiv biometric şi parolă).

6.2.7.1.1 Certificate calificate DigiSign

Standardul DigiSign pentru protecţia cheii private a certificatelor calificate este pentru ca abonaţii să:

- Folosească smartcard sau alt dispozitiv de hardware criptografic de securitate cu o putere echivalentă (dispozitivul creării de semnătura securizată), pentru a autentifica utilizatorul înainte de activarea cheii private;
- Să ia măsuri pentru protecţia fizică a staţiei de lucru a utilizatorului, pentru a preveni folosirea staţiei de lucru.

Se recomandă folosirea unei parole împreună cu un smartcard sau cu alt dispozitiv de hardware criptografic, în concordanţă cu punctul § 6.4.1.

6.2.7.2 Cheile private ale administratorilor

6.2.7.2.1 Administratorii

Standardul DigiSign pentru protecţia cheilor private ale administratorilor are următoarele cerinţe:

- Utilizarea unui smartcard, dispozitiv de acces biometric sau parolă, în conformitate cu CPP § 6.4.1 sau o măsură de securitate cu putere echivalentă pentru autentificarea administratorului înainte de activarea cheii private, care cuprinde, de exemplu, o parolă de operare a cheii private, parolă de intrare în sistemul Windows sau de screen saver sau o parolă de intrare în reţea;

Se recomandă pentru autentificarea administratorului, înainte ca acesta să activeze cheia privata, utilizarea unei parole împreuna cu un smartcard, un dispozitiv de acces biometric, în conformitate cu § 6.4.1 CPP.

6.2.7.3 Cheile private deţinute de DigiSign S.A.

Cheile private ale AC DigiSign sunt activate de un număr limitat de acţionari, care îşi furnizează datele (tokens sau passphrases), conform § 6.2.2. CPP. Pentru AC offline a DigiSign, cheia privată a AC este activată pentru o singură sesiune (ex: pentru certificarea unui AC subordonat sau pentru situaţia în care AC semnează o lista de revocare a certificatelor) după care, aceasta este dezactivată şi modulul se returnează în depozitul securizat. Pentru AC online DigiSign, cheia privată este activată pentru o perioada nedeterminată de timp, iar modulul rămâne online în centrul de producţie a datelor până când AC este scoasă offline (ex: pentru întreţinerea sistemului). Acţionarii DigiSign trebuie să-şi protejeze părţile secrete şi să semneze un act de recunoaştere a obligaţiilor (responsabilităţilor) pe care le au în calitate de acţionari.

6.2.8 Metoda dezactivării cheii private

Cheile private ale AC DigiSign se dezactivează prin dezactivarea dispozitivului hardware folosit. Cheile private ale AI DigiSign (utilizate pentru autentificarea aplicaţiei AI) se dezactivează prin închiderea sesiunii de lucru a sistemului. AI DigiSign trebuie să-şi delogheze staţiile de lucru în momentul închiderii sesiunii de lucru.

Cheile private ale administratorilor DigiSign, ale AI şi ale utilizatorilor finali pot fi dezactivate după fiecare operaţie, prin închiderea sesiunii de lucru a sistemului sau prin înlăturarea smartcard-ului din cititorul de smartcard, în funcţie de mecanismul de autentificare folosit de utilizator. În toate cazurile, utilizatorii finali au obligaţia de a-şi proteja în mod adecvat cheile private, în conformitate cu dispoziţiile 2.1.3, 6.4.1. CPP.

6.2.8 Metoda distrugerii cheii private

Atunci când se cere DigiSign S.A, distruge cheile private ale AC într-o maniera care să asigure faptul că nu au rămas resturi ale cheii care ar putea permite reconstituirea ei.

DigiSign S.A, utilizează funcţii de minimizare a modulului de hard criptografic şi alte mijloace pentru a asigura distrugerea completă a cheilor private ale AC. Activitatea de distrugere a cheilor private este urmărită.

6.3 Alte aspecte legate de managementul perechii de chei

6.3.1 Arhivarea cheii publice

AC DigiSign şi certificatele utilizatorilor finali sunt supuse procesului de salvare de siguranţă şi arhivate, aceasta constituind parte a procedurilor back-up.

6.3.2 Perioadele de utilizare a cheilor private şi publice

Perioada de valabilitate a unui certificat ia sfârşit prin expirarea (ajungere la termen) sau revocarea sa. Perioada de valabilitate a perechii de chei coincide cu perioada de valabilitate a certificatelor, dar cheile private pot fi folosite în continuare pentru decriptare, iar cheile publice, pentru verificarea semnăturii. Perioadele maxime de valabilitate ale certificatelor emise de DigiSign, după intrarea în vigoare a CPP, sunt prezentate în tabelul 10.

În plus, AC DigiSign încetează emiterea de noi certificate la o dată anterioară expirării certificatelor AC, astfel încât nici un certificat emis de un subordonat al AC nu expiră după expirarea certificatelor unui AC superior.

Certificate emise de:	*Certificate calificate DigiSign*	*Certificate clasa 3 CA*
AC root care se autosemnează (2048 bit)	N/A	Până la 20 ani
Public AC la AC (2048 bit)	N/A	Până la 10 ani
AC la utilizatori finali	Până la 2 ani	N/A

Tabelul 10 – **Perioadele de valabilitate ale certificatelor**

Prin excepţie de la cele reţinute în aceasta secţiune, participanţii vor înceta să utilizeze perechile de chei după ce perioadele lor de valabilitate au expirat.

Certificatele emise de AC pentru utilizatorii finali pot avea o perioadă de valabilitate mai mare de doi ani, de până la cinci ani, dacă sunt întrunite următoarele condiţii:

- Certificatele respective sunt certificate individuale;
- Perechile de chei ale abonaţilor se afla pe un token sau smartcard;
- Abonaţii se supun anual procedurilor de reautentificare, prevăzute în CPP § 3.1.9;
- Abonaţii vor face dovada anual că posedă cheia privată corespunzătoare cheii publice cuprinsă în certificat;
- Dacă un utilizator nu se reautentifică, în conformitate cu procedurile prevăzute în CPP § 3.1.9 sau nu poate face dovada că posedă tipul de cheie privată amintit anterior, AC îi va revoca în mod automat certificatul.

6.4 Datele de activare

6.4.1 Instalarea şi generarea datelor de activare

Datele de activare (părţile secrete), utilizate pentru protejarea smartcard-urilor ce conţin cheile private ale AC DigiSign, sunt generate, în conformitate cu dispoziţiile CPP § 6.2.2 privind ceremonia generării perechii de chei criptografice. Crearea şi distribuirea părţilor secrete este înregistrată.

AI DigiSign trebuie să selecteze parole puternice de protecţie a cheilor private. Principiile de bază ale operaţiei de selecţie a parolelor DigiSign impune ca parolele:

- să fie generate de utilizator;
- să aibă cel puţin opt caractere;
- să aibă cel puţin câte un caracter alfabetic şi câte unul numeric;
- să aibă cel puţin o literă mică;
- să nu cuprindă repetări a aceluiaşi caracter;
- să nu fie identică cu parola profilului operatorului;
- să nu conţină un subşir al profilului utilizatorului.

DigiSign recomandă ca administratorii, AI şi utilizatorii finali să-şi aleagă parole care întrunesc aceleaşi condiţii. De asemenea, DigiSign recomandă două mecanisme de

autentificare pentru activarea cheii private (ex. smartcard-uri şi parole, dispozitive biometrice şi smartcard-uri).

6.4.2 Protecţia datelor de activare

Acţionarii DigiSign S.A. trebuie să-şi protejeze părţile secrete şi să semneze un act de recunoaştere a obligaţiilor pe care le au în calitate de acţionari.

AI DigiSign trebuie să stocheze cheile private ale administratorului/AI, într-o formă criptată, utilizând parole de protecţie şi opţiuni de "înalta securitate"pentru browsere.

DigiSign S.A. recomandă insistent ca stocarea cheilor private a administratorilor, AI şi a utilizatorilor finali să se facă într-o formă criptată, iar protejarea cheilor private să se facă prin utilizarea de dispozitive hardware, de smartcarduri şi parole puternice. De asemenea, se încurajează recurgerea la două mecanisme de autentificare (ex. smart card-uri şi parole sau dispozitive biometrice şi smartcarduri).

6.5 Controlul securităţii computerelor

DigiSign S.A, execută toate funcţiile AC prin utilizarea sistemelor de încredere (Trustworthy Systems) care întrunesc cerinţele ghidului privind condiţiile de securitate şi verificare. De asemenea, DigiSign utilizează sistemele de încredere care întrunesc cerinţele ghidului privind securitatea întreprinderii .

6.5.1 Condiţii specifice privind securitatea tehnică a computerelor

DigiSign S.A asigură faptul că sistemele de întreţinere a software-ului şi fişierelor de date ale AC sunt sisteme de încredere securizate, pentru a preveni accesul neautorizat. În plus, DigiSign S.A, limitează accesul la server-ele de producţie doar acelor persoane, care au motive întemeiate pentru un astfel de acces. Utilizatorii aplicaţiilor generale nu au conturi la server-ele de producţie.

Reţeaua de producţie a DigiSign este separată logic de celelalte componente. Această separare previne accesul la reţea, cu excepţia accesului prin procesele de aplicaţii definite. Pentru protecţia reţelei de producţie de intruziunile din interior sau exterior şi pentru limitarea naturii şi sursei activităţilor din reţea, care ar putea duce la accesarea sistemele de producţie, DigiSign S.A utilizează firewall-uri.

DigiSign S.A. solicită utilizarea de parole, care să aibă un număr minim de caractere şi o combinaţie de caractere speciale şi alfanumerice. DigiSign S.A. solicită schimbarea periodică a parolelor.

Accesul direct la bazele de date care susţin registrul este limitat la persoanele de încredere, care au motive întemeiate pentru un astfel de acces.

6.5.2 Clasarea securităţii computerelor

Un echivalent al versiunii software-ului din centrul de procesare al DigiSign a satisfăcut condiţiile EAL 4 prevăzute de ISO/IEC 15408-3:1999, Tehnologia Informaţiei – *Tehnici de securitate –Criterii de evaluare pentru securitatea IT – Partea a 3-a: Condiţiile de securitate*, pe baza criteriilor comune de evaluare a software-ului, într-un laborator independent al centrului de procesare securizată al DigiSign. DigiSign poate, din când în când, să evalueze noile lansări de soft-uri ale centrului de procesare pe baza criteriilor comune.

6.6 Controlul tehnic al ciclului de viaţă

6.6.1 Controlul sistemului de dezvoltare

Aplicaţiile sunt dezvoltate şi implementate de Digisign S.A, în conformitate cu standardele sistemelor de dezvoltare şi managementului calitatii si securitatii informatiei. De asemenea,DigiSign dezvolta software-ul necesar activităţii AI şi anumitor funcţii ale AC. Acest tip de software este dezvoltat în conformitate cu standardele sistemelor de dezvoltare .

6.6.2 Controlul managementului securităţii

DigiSign S.A. poseda mecanisme şi/sau politici de punere în mişcare a controlului şi monitorizării configuraţiei sistemelor AC. DigiSign S.A. creează o funcţie hash pentru toate pachetele de soft şi soft-ul actualizat al DigiSign. Această funcţie hash se utilizează pentru verificarea manuală a integrităţii acestor tipuri de soft. Periodic, după instalare, DigiSign S.A. validează integritatea sistemelor AC.

6.7 Controlul securităţii reţelei

DigiSign S.A execută funcţiile AC sau prin utilizarea de reţele securizate, în conformitate cu ghidul condiţiilor de securitate şi audit, pentru a preveni accesul

neautorizat şi alte activităţi ilegale. DigiSign S.A. îşi protejează comunicarea informaţiilor sensibile, prin utilizarea criptării şi semnăturilor digitale.

6.8 Controlul modulelor criptografice

Modulele criptografice utilizate de DigiSign întrunesc condiţiile prevăzute în cap. § 6.2.1. al CPP.

7. Profilul certificatelor şi al LCR (lista certificatelor revocate)

7.1 Profilul certificatelor

Cap.§ 7.1 CPP defineşte condiţiile profilelor şi conţinutului certificatelor DigiSign, condiţii care trebuiesc îndeplinite de certificatele emise în baza acestui CPP.

Certificatele DigiSign se conformează recomandărilor X.509 (19970 (a) ITU-T): Tehnologia Informaţiei – Interconexiunile sistemelor deschise - directorul: Schema autentificării, iunie 1997 şi (b) RFC 2459: Internet X.509 Infrastructura cheii publice a certificatului şi profilul CRL, ianuarie 1999 ("RFC 2459") (c) Legea romana privind certificatele calificate (d) standardele Uniunii Europene privind certificatele calificate.

Certificatele X.509 DigiSign conţin domeniile X.509 versiunea 3 şi valorile prescrise sau obligatorii din tabelul 11, de mai jos:

Profilul certificatului	
Domeniu	***Valoare sau valoare obligatorie***
Versiune	Certificatele AC DigiSign S.A. şi ale abonaţilor utilizatori finali sunt certificate de tipul X.509 versiunea 3
Număr serie	Valoare unică pe emitent DN
Algoritmul semnăturii	Certificatele AC DigiSign S.A. folosesc algoritmul sha1RSA iar ale abonatilor utilizatori folosesc algoritmul sha1RSA
Emitent DN	CN = DIGISIGN PUBLIC OU = DIGISIGN Public CA

	O = DIGISIGN S.A. C = RO
Valabil de la	Bazat pe coordonatorul de timp universal sincronizat cu ceasul principal al Observatorului Naval al U.S.A., codificat în conformitate cu RFC 2459.
Valabil până la	Bazat pe coordonatorul de timp universal sincronizat cu ceasul principal al Observatorului Naval al U.S.A., codificat în conformitate cu RFC 2459. Perioada de valabilitate va fi stabilită în conformitate cu prevederile obligatorii specificate în cap. § 6.3.2. CPP
Subiectul DN	E =adresa de e-mail a subiectului CN = Numele subiectului O = Societatea OU = Functia – functia subiectului C = tara (de ex. RO)
Cheia Publica	RSA(1024) sau RSA (2048)
Extensiile certificatului	
Domeniu	***Valoare sau valoare obligatorie***
Utilizarea cheii	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0) (extensiile de utilizare a certificatului conform standardului X.509 versiunea 3)
Utilizarea extinsa a cheii	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document signing (1.3.6.1.4.1.311.10.3.12) Time Stamping (1.3.6.1.5.5.7.3.8)

	Smart Card Logon (1.3.6.1.4.1.311.20.2.2) (utilizarea extinsa a certificatelor conform standardului X.509 versiunea 3)
Politicile certificatului	[1]Certificate Policy: Policy Identifier=Secure Signature Creation Device Qualified Certificate (0.4.0.1862.1.4) [2]Certificate Policy: Policy Identifier=European Qualified Certificate (0.4.0.1862.1.4) [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.311.21.8.9830102.4854409.15286941.299836.13424610.9.11247277.10779323 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digisign.ro/products-and-services/security-services/qualified-certificates/index.html
Numele alternativ al subiectului	RFC822 Name= denumirea utilizatorului de windows al subiectului Other Name: Principal Name= denumirea utilizatorului de windows al subiectului (Aceasta extensie este folosita pentru logarea pe domeniu de Windows)
Subject key identifier	Identificator conform RFC Internet X.509, privind cheia publica a certificatului utilizatorului final.
Authority key identifier	Identificator conform RFC Internet X.509, privind cheia publica a AC semnatare
Constrangeri de baza	Subject Type=End Entity Path Length Constraint=None
Punctele de distributie ale LCR	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.digisign.ro/Qualified/latest.crl
Tipul certificatului	SSL Client Authentication (80)

pentru Netscape	

Tabelul 11 – Profilul certificatelor

7.1.1 Numărul versiunii

- Certificatele AC DigiSign S.A. şi ale abonaţilor utilizatori finali sunt certificate de tipul X.509 versiunea 3.

7.1.2 Extensiile certificatelor

Când sunt utilizate certificatele X.509 versiunea 3, DigiSign completează certificatele cu extensiile prevăzute in tabelul de mai sus.

7.1.2.1 Utilizarea cheii

Certificatele calificate DigiSign pot utiliza extensiile "Key Usage", tabelul de mai sus.

7.1.2.2 Politicile privind extensiile certificatelor

Certificatele calificate DigiSign utilizează extensia "Certificate Policies". Politicile certificatelor sunt prezentatea in tabelul de mai sus

7.1.2.3 Constrângeri de bază

DigiSign S.A. completează certificatele X.509 versiunea 3 ale AC cu extensia "Basic Constraints", "Subject Type" setat AC. Certificatele utilizatorilor finali sunt completate cu extensia "Basic Constraints", "Subject Type" fiind entitatea finală.

Certificatele X.509 versiunea 3 emise de AC DigiSign vor avea domeniul "pathLenConstraint" al extensiei "Basic Constraints" setat la numărul maxim de certificate ale AC, care trebuie să urmeze acest certificat într-o cale de certificare. Certificatele AC emise online pentru AC şi DigiSign care emite certificate utilizatorului final are câmpul "pathLenConstraint" setat la valoarea "none", fapt ce indică că numai un utilizator final poate urma în calea de certificare.

7.1.2.4 Punctele de distribuire ale LCR

Punctele de distribuire ale LCR se găsesc la adresa:
http://crl.digisign.ro/Qualified/latest.crl

Utilizarea punctelor de distribuire ale LCR vor putea fi susţinute de AC DigiSign în viitor.

7.1.2.5 Identificator pentru cheia publică a autorităţii

KeyID=a8 1c ec d2 5b 21 4b 5f 7b 11 c0 6e 53 c7 78 26 eb 5b bd 52

7.1.2.6 Identificatorul cheii subiectului

37 b3 d5 f2 ce 9d e6 1b 46 e8 65 b8 ad 2e d5 9e 5c 69 0e dd.

7.1.2.7 Identificatorii algoritmului unui obiect

AC DigiSign foloseşte algoritmul sha1 .

7.1.3 Formele numelui

DigiSign completează certificatele cu numele (denumirea) emitentului şi numele caracteristic al subiectului sau numele organizaţiei, după caz, în conformitate cu cap. § 3.1.1.CPP.

7.2 Profilul LCR

DigiSign S.A. emite LCR-uri în conformitate cu RFC 2459. LCR-urile DigiSign S.A. au următorul conţinut şi domenii de bază, specificate în tabelul 12, de mai jos:

Domeniu	*Valoare sau valori obligatorii*
Versiune	A se vedea cap. §7.2.1CPP.
Algoritmul semnăturii	Algoritmul folosit la semnarea LCR. LCR-urile DigiSign se semnează folosind sha1RSA (OID: 1.2.840.113549.1.1.4) sau md2RSA (OID: 1.2.840.113549.1.1.2), în conformitate cu RFC 2459.
Emitent	Entitatea care a semnat şi emis LCR.
Data intrării în	Data emiterii LCR. LCR-urile DigiSign intră în vigoare la data

Domeniu	*Valoare sau valori obligatorii*
vigoare	emiterii.
Certificate revocate	Lista certificatelor revocate, inclusiv numărul serial al certificatelor revocate şi data revocării.

Tabelul 12 – Câmpurile de baza ale profilurilor LCR

7.2.1 Numărul versiunii

DigiSign S.A. emite în mod curent LCR X. 509 versiunea 2.

8. Administrarea specificaţiilor

7.3 Procedurile de modificare a specificaţiilor

Amendamentele la acest CPP vor fi făcute de DigiSign S.A. Ele vor avea forma unui document care cuprinde modificări sau actualizări ale CPP. Aceste variante vor fi accesate la secţiunea de "Actualizări şi completări ale Codului de practici şi proceduri" , care este localizată la adresa:

http://www.digisign.ro/ro/footer/codul_de_practici_si_proceduri

Actualizările elimină orice dispoziţie conflictuală a CPP-ului de referinţă.

7.3.1 Aspecte care pot fi schimbate fără înştiinţare prealabilă

DigiSign S.A. îşi rezervă dreptul de a aduce modificări de formă dispoziţiilor CPP, fără notificare prealabilă, inclusiv corectarea greşelilor de tipar, schimbări de URL şi a informaţiilor de contact. Deciziile DigiSign, care au ca obiect desemnarea amendamentelor ca fiind modificări de formă sau de fond, rămân la discreţia acesteia.

7.3.2 Probleme care pot fi modificate cu înştiinţare prealabilă

DigiSign S.A. va opera modificările dispoziţiilor de fond ale CPP în conformitate cu cap. § 8.1.2. CPP.

8.1.2.1 Lista problemelor

Modificările de fond, în înţelesul dispoziţiilor cap. § 8.1.1 CPP, sunt acelea pe care DigiSign le consideră fiind astfel.

8.1.2.2 Mecanismul înştiinţării

Colectivul de lucru al dezvoltării practicilor DigiSign va face propuneri de modificări ale CPP în secţiunea de "Actualizări şi completări a codului de practici şi proceduri" aflată în registrul DigiSign SA, localizat la: http://www.digisign.ro/ro/footer/codul_de_practici_si_proceduri. DigiSign va cere celorlalţi participanţi să facă propuneri de modificări la CPP. Dacă DigiSign S.A. consideră că aceste propuneri sunt oportune şi intenţionează să le implementeze, le va semnala conform procedurii din această secţiune.

Prin excepţie de la dispoziţiile CPP, dacă DigiSign S.A. consideră că modificările de fond se impun de urgenţă, pentru a împiedica sau stopa încălcarea securităţii, DigiSign S.A. are mandat să formuleze astfel de amendamente, publicându-le în registrul DigiSign. Acestea vor intra în vigoare imediat de la data publicării lor.

8.1.2.3 Perioada comentariilor

Prin derogare de la dispoziţiile § 8.1.2.2 CPP, comentarea oricărui amendament de fond la CPP va fi de cincisprezece (15) zile, începând cu data de la care acesta a fost trimisă în registrul DigiSign. Participanţii DigiSign S.A. pot să-şi păstreze aceste amendamente până la sfârşitul acestei perioade.

8.1.2.4 Mecanismul de gestionare a comentariilor

Colectivul de lucru al dezvoltării practicilor DigiSign va lua în considerare toate comentariile la propunerile de amendamente. DigiSign S.A. va proceda, fie (a) permiţând ca propunerile să intre în vigoare fără amendamente, fie (b) modificând aceste propuneri, apoi republicându-le sub formă de noi amendamente, în conformitate cu dispoziţiile cap. § 8.1.2.2 CPP, fie (c) retrăgând aceste propuneri de amendamente. DigiSign S.A. are dreptul să retragă aceste amendamente prin înscrierea acestora în secţiunea de "Actualizări şi completări ale codului de practici şi proceduri" din registrul DigiSign S.A. Cu excepţia celor propuse sau retrase, amendamentele (modificările) vor intra în vigoare la data expirării perioadei de valabilitate a comentariilor, în conformitate cu cap. § 8.1.2.3.CPP.

7.4 Publicarea politicilor

7.4.1 Documente care nu se publică în CPP

Documentele de securitate, care sunt considerate confidențiale de DigiSign, nu se dezvăluie publicului. Documentele de securitate confidențiale sunt cele identificate în cap. § 1.1(a) tabelul 1 CPP, ca fiind inaccesibile publicului.

7.4.2 Distribuirea CPP

Acest CPP este publicat în formă electronică în registrul DigiSign S.A., la **http://www.digisign.ro/uploads/cpp.pdf**

CPP este disponibil în format Adobe Acrobat. De asemenea, DigiSign S.A. pune la dispoziție CPP, în format Adobe Acrobat pdf, la cerere, trimisă la **cpp@digisign.ro**. CPP este disponibil în formă tipărită de colectivul de lucru al dezvoltării de practici DigiSign, la cerere, trimisă la adresa:

DigiSign S.A.

Str. Virgil Madgearu, Nr. 2-6, sector 1, București

Attn: CPP.

Acronime şi definiţii

Acronim	*Termen*
ANSI	Institutul American de Standarde Naţionale.
B2B	Business-to-business.
AC	Autoritate de Certificare
CPP	Codul de Practici şi Proceduri.
LCR	Lista Certificatelor Revocate.
EAL	Nivelul de asigurare al evaluării (conform Criteriilor Comune).
FIPS	Standardele Federale de Procesare a Informaţiei ale Statelor Unite.
ICC	Camera Internaţionala de Comerţ
LSVA	Evaluarea vulnerabilităţii securităţii logice
PIN	Număr personal de identificare.
PKCS	Standardul de criptare a cheii publice.
PKI	Infrastructura cheii publice.
AI	Autoritate de înregistrare.
RFC	Cerere pentru comentarii.
SSL	Secure Sockets Layer.
S/MIME	Extensii de securitate mail Internet în scopuri multiple.

Definiţii

Termen	*Definiţie*
Ghidul securităţii companiei	Un document care stabileşte condiţiile şi practicile de securitate pentru clienţii DigiSign.

Termen	Definiţie
Ghidul privind ceremonia cheii	Documentul care descrie procedeele şi cerinţele ceremoniei de generare a cheii.
Politica de securitate a	Document de maxima importanţă care descrie politicile de securitate ale DigiSign.
Administrator	O persoană de încredere, care desfăşoară activităţi de validare şi oricare alte funcţii ale AC sau AI.
Certificatul administratorului	Certificatul emis pentru uzul administratorului, care poate fi folosit doar pentru desfăşurarea funcţiilor AC sau AI.
Administrare automată	Procedura prin care cererile de eliberare de certificate se aprobă automat, dacă informaţia furnizată la înscriere se verifică cu cea aflată în baza de date.
Certificat	Un mesaj care specifică numele sau identifică AC, semnatarul, conţine cheia publică a semnatarului, stabileşte perioada de valabilitate a certificatului, conţine numărul serial al certificatului şi este semnat digital de către AC.
Solicitantul certificatului	O persoană fizică sau juridică, care solicită emiterea unui certificat de către AC.
Solicitarea certificatului	O cerere formulată de către solicitant sau de către persoana împuternicită de către solicitant, adresata AC, în vederea emiterii unui (unor) certificat(e).
Lanţul certificatelor	O listă ordonată de certificate, care conţine certificatul semnatarului şi certificatele AC, care se termină în certificatul de bază.
Certificat de administrare a obiectivelor de control	Criteriile pe care o entitate trebuie să le întrunească pentru a satisface auditul de conformitate.
Lista certificatelor revocate (LCR)	O listă emisă periodic (sau în mod extraordinar), semnată digital de către AC, care identifică certificatele care au fost revocate înainte de expirarea perioadei de

Termen	Definiţie
	valabilitate a acestora. În general, lista indică numele (denumirea) emiţătorului LCR, data emiterii ei, data programării emiterii următoarei LCR, numărul serial al certificatelor revocate, data şi motivele revocării.
Cerere pentru semnarea certificatului	Mesajul care transmite cererea pentru emiterea certificatului.
Autoritate de certificare (AC)	Entitatea autorizată să emită, administreze, revoce şi sa reînnoiască certificate.
Codul de practici şi proceduri (CPP)	Practicile şi procedurile pe care DigiSign S.A. le aplică în activitatea de aprobare sau respingere a cererilor de eliberare de certificate, emitere, administrare şi revocare a certificatelor. În contextul acestui CPP, "CPP" se referă la acest document.
Parola de verificare	Parola secretă care este aleasă de solicitant atunci când face o cerere de înscriere pentru obţinerea de certificate. Atunci când este emis certificatul, solicitantul capătă calitatea de semnatar şi AC poate folosi aceasta parolă de verificare la autentificarea semnatarului, când acesta vrea să revoce sau să reînnoiască certificatul.
Auditul de conformitate	Procesul de verificare periodică, căruia DigiSign S.A. trebuie să i se supună, pentru a se determina dacă acestea se conformează standardelor europene.
Compromis	O violare a politicii de securitate, prin care s-ar putea produce o dezvăluire neautorizată, o pierdere de control asupra informaţiei sensibile. Din perspectiva cheilor private, compromis înseamnă pierdere, furt, dezvăluire, modificare, folosire neautorizată sau alt compromis asupra securităţii cheii private.
Informaţie	Informaţia care trebuie păstrată confidenţial şi privat, potrivit dispoziţiilor cap. § 2.8.1 CPP.

Termen	Definiţie
confidenţială/privată	
Acordul privind modul de utilizare a LCR	Acordul prin care se stabilesc termenii şi condiţiile în care poate fi folosită o LCR sau informaţia cuprinsă în ea.
Politica de securitate a DigiSign	Un document de maximă importanţă care descrie politicile de securitate ale DigiSign.
Drepturile de proprietate intelectuală	Drepturile asupra unuia sau mai multora din următoarele: drepturi de autor, brevete de invenţii, secrete de fabricaţie, mărci şi alte drepturi de proprietate.
Autoritate de certificare intermediară (AC Intermediar)	Autoritatea de certificare ale cărei certificate sunt localizate intr-un lanţ de certificate, între certificatul bazei AC şi certificatele autorităţii de certificare care emite certificatele semnatarului utilizator final.
Ceremonia de generarea a cheii	O procedură prin care perechea de chei a unui AC sau AI este generată, transferată într-un modul criptografic, este salvată şi/sau este certificată.
Autenticarea manuală	Procedura prin care cererile pentru certificate sunt revizuite şi aprobate manual, una cate una, de către un administrator, prin utilizarea unei interfeţe web.
Informaţia neverificată a semnatarului	Informaţia furnizată de către un solicitant al certificatului autorităţii de certificare şi care este cuprinsă în certificat, care nu a fost confirmată de AC şi pentru care AC nu garantează decât că informaţiile au fost trimise de solicitantul de certificat.
Non-repudierea	Un atribut al comunicaţiei care asigură protecţia împotriva unei părţi care neagă originea şi faptul că a trimis cererea pentru certificat sau neagă livrarea acestuia. Negarea originii cuprinde negarea faptului că această comunicare provine din aceeaşi sursă a mesajelor anterioare, chiar dacă identitatea asociată cu

Termen	Definiţie
	expeditorul este necunoscută. Notă: numai instanţa de judecată sau un tribunal arbitrar pot împiedica în cele din urma repudierea.
Perioada de valabilitate	Perioada cuprinsă între data emiterii certificatului (sau o dată ulterioară, dacă se specifică astfel în certificat) şi data expirării valabilităţii acestuia, sau o dată anterioară termenului de expirare, în situaţia în care certificatul este revocat.
PKCS #10	Standardul de criptare a cheii publice #10, dezvoltat de către RSA Security Inc., care defineşte structura unei cereri de semnare a certificatului.
PKCS #12	Standardul de criptare a cheii publice #12, dezvoltat de către RSA Security Inc., care defineşte mijloacele de securitate pentru transferul cheilor private.
Infrastructura cheii publice (PKI)	Arhitectura, organizarea, tehnicile, practicile şi procedurile care susţin în mod colectiv implementarea şi operarea sistemului criptografic al cheii publice de generare a certificatului.
Certificat cu amănuntul	Certificatul emis de către DigiSign, comportând-se ca AC, persoanelor fizice sau juridice, care aplică, unul câte unul, pe web site-ul DigiSign S.A.
RSA	Sistemul criptografic al cheii publice, inventat de Rivest, Shamir şi Adelman.
Secret Share (partea secretă)	O porţiune a cheii private a AC sau o porţiune a datelor de activare necesare operării cheii private a AC, în baza aranjamentului Secret Sharing.
Secret Sharing	Procedeul de împărţire a cheii private a AC sau a datelor de activare pentru operarea cheii private a AC, astfel încât să permită un control multi-personal asupra operaţiunilor cheii private a AC, în baza dispoziţiilor cap. § 6.2.2. CPP.

Termen	Definiție
Subiect	Deținătorul cheii private, care corespunde cheii publice. Termenul de "subiect", în cazul certificatelor emise persoanelor juridice, se poate referi la echipamentul sau dispozitivul care păstrează cheia privată. Subiectului îi corespunde un nume concret, care este legat de cheia publică cuprinsă în certificatul subiectului.
Semnatar	În cazul certificatelor emise persoanelor fizice, persoana respectivă este subiectul certificatului. În cazul persoanelor juridice, subiectul este compania care deține echipamentul sau dispozitivul şi căreia i s-a emis certificatul. Un semnatar poate să folosească, şi are această autorizare, cheia privată care corespunde cheii publice cuprinsă în certificat.
Contractul semnatarului (Subscriber Agreement)	Un acord folosit de AC, care stabileşte termenii şi condițiile în care o persoană fizică sau juridică dobândeşte calitatea de semnatar.
Supplemental Risk Management Review(Verificarea suplimentară asupra managementului riscului)	Verificarea unei entități, ca rezultat al constatărilor nemulțumitoare din raportul de verificare asupra procesului de management al riscului desfăşurat de acea entitate.
Vânzător	O entitate care desfăşoară servicii de vânzare în numele DigiSign.
Persoana de încredere	Un angajat, contractant sau consultant al unei entități, care are responsabilități privind administrarea infrastructurii de încredere a acelei entități, produsele, serviciile, facilitățile şi/sau practicile acelei entități, aşa cum au fost definite în cap. § 5.2.1 CPP.

Termen	*Definiţie*
Funcţia (postul) de încredere	Poziţia pe care trebuie să o aibă o persoană de încredere.
Sistem de încredere	Partea hardware, software şi procedurile care sunt securizate în mod rezonabil împotriva intruziunilor şi abuzurilor; furnizează un nivel rezonabil de disponibilitate, încredere şi operare corectă; sunt potrivite pentru desfăşurarea funcţiilor pentru care au fost programate; sunt compatibile cu politicile de securitate.
Registrul DigiSign S.A.	Baza de date a certificatelor DigiSign şi a altor informaţii relevante, accesibile on-line.
Politica de securitate a DigiSign S.A.	Document de maximă importanţă, care descrie politicile de securitate ale DigiSign.
Participanţii DigiSign S.A.	O persoană fizică sau juridică, care poate avea, în raport cu DigiSign, una sau mai multe din calităţile următoare: DigiSign, vânzător, semnatar.

Actualizari

N	Versiunea in vigoare	Data
1	1.0	01.06.2005
2	1.1	15.06.2005
3	1.2	01.08.2005
4	1.3	10.08.2005
5.	1.4	01.10.2008
6.	1.5	04.01.2010