Politica de Certificare

DigiSign

Versiunea 1.0

10.08.2015

DigiSign S.A.

Str. Virgil Madgearu, Nr. 2-6, Sector 1

014135, București, România

031 620 12 89

www.digisign.ro

DigiSign S.A. Str. Virgil Madgearu nr. 2-6, București, Sector 1, 014135, România Tel: 031 620 12 84, Fax: 031 620 12 91, office@digisign.ro www.digisign.ro

Cuprins

Observații preliminare

DigiSign S.A.

Str. Virgil Madgearu, Nr. 2 - 6, Sector 1

014135, București, România

Tel: 031 620 12 84

Fax: 031 620 20 99

e-mail: cp@digisign.ro

1. Introducere

Prezentul document poartă numele **Politica de Certificare** (denumită în continuare **CP**) și descrie regulile și principiile de bază aplicate de **DigiSign** în procesul de furnizare a serviciilor de certificare. O descriere detaliată a întregului proces de certificare este prezentată în **Codul de Practici și Proceduri DigiSign**.

Toate documentele referitoare la procesele desfășurate de către DigiSign, în vederea furnizării serviciilor de certificare, se regăsesc în secțiunea *Documente*, pe site-ul propriu: www.digisign.ro. Informațiile publicate de DigiSign prin interfața online a site-ului www.digisign.ro, au caracter public și nu sunt necesare drepturi speciale pentru accesarea acestora.

Politica de Certificare DigiSign se aplică societății DigiSign S.A. ca Autoritate de Certificare – AC, Autoritate de Înregistrare – AI, Autoritate de Validare – AV, precum și oricăror altor autorități aflate în relație de subordonare sau aflate într-o relație contractuală cu societatea DigiSign S.A.

Acest document descrie regulile și principiile generale pe care furnizorul de servicii de certificare DigiSign le respectă pentru a emite, reînnoi, suspenda, revoca și administra certificatele digitale, în conformitate cu prevederile legale în materie, și anume:

- ✓ Legea Nr. 455/2001 privind semnătura electronică;
- ✓ Legea Nr. 451/2004 privind marca temporală;
- ✓ Hotărârea Guvernului Nr. 1259/2001 privind aprobarea Normelor Tehnice și Metodologie de Aplicare a Legii Nr. 455/2001 privind semnătura electronică, cu modificările și completările ulterioare;
- ✓ Ordinul Ministrului Comunicațiilor și Societății Informaționale Nr. 492/2009 privind Normele Tehnice și Metodologice pentru Aplicarea Legii Nr. 451/2004 privind marca temporală;
- ✓ Ordinul Ministrului Comunicațiilor și Societății Informaționale nr. 850/08.08.2011 privind calitatea de furnizor acreditat de servicii de certificare dobândită de societatea DigiSign S.A;
- ✓ Directiva 1999/93/EC a Parlamentului European și a Consiliului European încheiată la 13 decembrie 1999 privind stabilirea cadrului comunitar pentru semnătura electronică, cu modificările și completările ulterioare;
- ✓ Recomandările Internet Engineering Task Force:
  - RFC 3647 – „Internet X.509 Public Key Infrastrucuture Certificate Policies and Certification Practices Framework;
- ✓ Standardul ISO/IEC 27002 – Code of Practice for Information Security Management;
- ✓ Standardul ETSI TS 101456 – „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates”;
- ✓ Standardul ETSI TS 102042 – „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”;
- ✓ Standardul ETSI TS 102023 – „Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities”.

Politica de Certificare DigiSign stabilește regulile generale care guvernează asupra procesului de certificare, atât din perspectiva Autorităților de Certificare și Înregistrare, cât și din perspectiva utilizatorilor - Abonați și Entități Partenere.

2. Servicii de certificare

DigiSign, membră a grupului iNES, este furnizor acreditat de servicii de certificare din Romania, conform Ordinului Ministrului Societății Informaționale nr. 441/23.07.2014. Serviciile de certificare acreditate sunt dezvoltate de către profesioniștii din cadrul DigiSign, fiind proiectate special pentru necesitățile specifice ultimelor dezvoltări din domeniul securității informatice.

Certificatele digitale emise de fiecare Autoritate de Certificare DigiSign sunt încadrate în diferite clase, în funcție de nivelul de încredere al Autorității de Certificare Emitentă, fiind destinate atât utilizatorilor, cât și entităților partenere care doresc verificarea semnăturilor electronice aplicate cu aceste certificate.

DigiSign emite certificate digitale pentru orice entitate solicitantă în limitele prevederilor legale. Entitățile participante la procesul de certificare sunt: Autoritățile de Înregistrare, Autoritățile de Certificare și Autoritățile de Validare din cadrul DigiSign, pe de o parte, și utilizatorii finali – Abonații și Entități Partenere, pe de altă parte.

Toate autoritățile care întreprind acțiuni de înregistrare, certificare și validare în cadrul DigiSign sunt prezentate detaliat din punct de vedere legal, comercial și tehnic în *Codul de Practici și Proceduri DigiSign*, iar autoritățile care întreprind acțiuni de marcare temporală sunt descrise în propriul CPP, și anume: *Codul de Practici și Proceduri al Autorităților de Marcare Temporală DigiSign*.

Denumirea de Abonat (eng. *End User*) îi este atribuită oricărei entități care deține un certificat digital emis de o Autoritate de Certificare DigiSign și reprezintă acea entitate al cărei identificator se regăsește în câmpul *Subiect* al certificatului digital emis pentru acesta și care nu emite certificate altor entități.

Entitatea Parteneră (eng. *Third Party*) reprezintă orice entitate care utilizează certificatul digital al unui Abonat pentru a verifica semnătura electronică asociată acestuia, în vederea acceptării sau respingerii respectivului certificat.

DigiSign, ca furnizor de servicii de certificare acreditat, oferă diverse produse și servicii PKI, precum: înregistrare, emitere, reînnoire, suspendare și revocare, depozitare si publicare, marcare temporală și verificare online a stării certificatelor fie prin intermediului protocolului OCSP, fie prin intermediul Listei de Certificate Revocate (CRL).

Fiecare serviciu oferit are la bază un set de practici și proceduri descrise detaliat în CPP și sumarizate în prezentul document, după cum urmează:

- Înregistrarea cererilor pentru certificatele digitale este procesul care precedă emiterea acestora și presupune verificarea și autentificarea identității unui solicitant, precum și validarea cererii înaintate de către respectivul solicitant. Descrierea detaliată a procesului de înregistrare este redată în *Codul de Practici și Proceduri DigiSign, Capitolul 4 – Identificarea și autentificarea*.

- Emiterea certificatelor digitale reprezintă acea acțiune prestată de către Autoritățile de Certificare din cadrul DigiSign, care emit certificate digitale pentru orice entitate solicitantă, conform prevederilor legale. Descrierea detaliată a procesului de emitere este redată în *Codul de Practici și Proceduri DigiSign, Capitolul 5.3 – Emiterea certificatelor*

- Reînnoirea certificatelor digitale reprezintă acea acțiune prestată de către Autoritățile de Certificare din cadrul DigiSign oricărui Abonat care deține un certificat digital și o pereche de chei valide și dorește emiterea unui nou certificat digital. Descrierea detaliată a procesului de reînnoire este redată în *Codul de Practici și Proceduri DigiSign, Capitolul 5.6 – Reînnoirea sau modificarea certificatului*.

  De asemenea, DigiSign oferă utilizatorilor care dețin un certificat digital a cărui perioada de valabilitate a expirat, posibilitatea de a fi reemis prin procesul de reînnoire a cheilor. Întregul proces este descris în cadrul *Capitolului 5.7 – Reînnoirea cheilor* din *Codul de Practici și Proceduri DigiSign*.

- Revocarea unui certificat digital reprezintă procesul de anulare a validității acestuia și retragerea oricărui drept de al utiliza. Acest proces este realizat conform *art. 23* din *Legea nr. 455/2001 privind semnătura electronică,* fiind descris detaliat în *Codul de Practici și Proceduri DigiSign, Capitolul 5.8.1. – Revocarea unui certificat*.

- Suspendarea unui certificat digital reprezintă o revocare reversibilă a acestuia, fiind realizată conform *Legii nr. 455/2001 privind semnătura electronică.* Întregul proces de suspendare al unui certificat digital, precum și condițiile în care se realizează acest proces, sunt descrise în cadrul *Codului de Practici și Proceduri DigiSign, Cap. 5.8.2. – Suspendarea unui certificat digital*.

- Depozitarea și publicarea certificatelor digitale este realizată imediat acceptării unui certificat digital de către titularul acestuia. Depozitarea se face în cadrul *registrului electronic de certificate digitale,* care reprezintă sursa informațională de bază pentru toți participanții la procesul de certificare, fiind în permanență accesibil la adresa www.digisign.ro.

- Marcarea Temporală este un serviciu adițional oferit de către Autoritatea de Marcare Temporală din cadrul DigiSign și care confirma existența unor date in format electronic, într-o anumită formă dată, la un moment de timp determinat. Descrierea procesului de marcare temporală este detaliată în *Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign*.

- Serviciul de verificare online a stării certificatelor digitale prin intermediul protocolului OCSP este un serviciu conex oferit de către Autoritățile de Certificare DigiSign. Prin intermediul acestui serviciu sunt furnizate informații în timp real cu privire la starea unui certificat, în momentul în care serverul OCSP este interogat. Descrierea detaliată a procesului de verificare online a stării certificatelor este redată în *Codul de Practici și Proceduri DigiSign, Capitolul 8.4 – Profilul OCSP*.

- Serviciul de verificare a stării certificatelor digitale prin publicarea Listei de Certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogări HTTP, este un serviciu conex oferit de către Autoritățile de Certificare DigiSign pentru a oferi informații în timp util despre starea unui certificat digital – suspendat sau revocat. Descrierea detaliată a procesului de verificare online a stării certificatelor este redată în *Codul de Practici și Proceduri DigiSign, Capitolul 8.3 – Profilul CRL.*

3. Certificate digitale

Un Certificat digital reprezintă o suită de informații și atribute în format electronic, care leagă datele de semnare și verificare de o entitate și care confirmă identitatea acesteia.

Supus legislației în vigoare, un certificat digital emis de o Autoritate de Certificare DigiSign poate fi utilizat, fiind perfect valid, indiferent de locul în care se întreprind acțiuni cu acesta. De asemenea, certificatele digitale furnizate de către DigiSign au scopuri generale, putând fi utilizate la nivel global.

DigiSign nu limitează utilizarea certificatelor digitale emise la un anumit mediu de afaceri, cum ar fi un program pilot, un sistem de servicii financiare sau un mediu de piață virtuală. Cu toate acestea, DigiSign nu este responsabilă pentru monitorizarea sau impunerea unor anumite restricții de utilizare a certificatelor digitale în aceste medii.

Aria de aplicabilitate a certificatelor digitale emise de către Autoritățile de Certificare DigiSign acoperă următoarele utilități:

- ✓ autentificarea;
- ✓ semnarea (extinsă) electronică;
- ✓ non-repudierea datelor;
- ✓ confidențialitatea datelor;
- ✓ integritatea datelor;
- ✓ criptarea sau decriptarea datelor;
- ✓ verificarea unei semnături (extinse) electronice;
- ✓ validarea online a stării certificatelor prin intermediul protocolului OCSP;
- ✓ marcarea temporală.

DigiSign poate personaliza, la solicitarea utilizatorului, extensia unui certificat digital emis, astfel încât acesta să poate fi utilizat pentru semnarea de cod, autentificarea server Web, MS Smart Card Logon, MS Document Signing, Internet Key Exchange for Ipsec, MS Encrypted File System (EFS), Time Stamping, OCSP Signer.

DigiSign furnizează următoarele tipuri de certificate digitale, având arii diferite de aplicabilitate:

- Certificat digital Simplu – creează o semnătura electronică simplă (neextinsă) și permite semnarea e-mail-urilor și a fișierelor, precum și autentificarea unui abonat;

- Certificat digital Calificat – creează o semnătură electronică extinsă (în înțelesul dat de Legea 455/2001 privind semnătura electronică), asigură identitatea titularului și poate fi utilizat pentru securizarea tranzacțiilor online, a autentificării pe diferite portale, criptare, marcare temporală, semnarea e-mail-urilor și a fișierelor;
- Certificat digital pentru Criptare – utilizat pentru a asigura o securitate sporită a confidențialității datelor transmise sau primite;
- Certificat digital pentru Semnare de Cod – este utilizat pentru a proteja software-ul împotriva falsificării;
- Certificat digital pentru Confirmarea Autenticității Serverelor – utilizate de serviciile care operează pe baza protocoalelor SSL/TLS/WTLS;
- Certificat digital pentru Confirmarea Stării unui Certificat – utilizate de serverele care funcționează conform protocolului OCSP și care furnizează informații despre starea certificatelor digitale emise;
- Certificatele digitale ale Autorităților de Marcare Temporală – utilizate de serverele care, ca răspuns la cererea unui Abonat, emit mărci temporale prin care asociază unor date, fie ele documente, mesaje, semnături electronice etc, un moment de timp pe baza căruia se poate determina secvențialitatea în timp a datelor;
- Certificatele digitale ale Autorităților de Certificare – utilizarea acestora nu este restricționată la aria definită, aplicabilitatea lor fiind dată de extensia din certificate care stabilește modul în care va fi folosită cheia lor privată (vezi *Capitolul 8.2.4 - Certificate*).

În general, un certificat digital emis de către una din Autoritățile de Certificare DigiSign poate fi utilizat doar în scopul exprimat în cererea de emitere a acestuia și numai conform extensiei folosite pentru generarea respectivului certificat. Nivelul de sensibilitate al informațiilor până la care se dorește a se proteja sau autentifica date, trebuie evaluat de către utilizator. Acest nivel de sensibilitate stă la baza deciziei de a alege și a solicita unul din tipurile de certificate digitale furnizate de către DigiSign. În acest mod se delimitează aria de aplicabilitate a fiecărui tip de certificat. Spre exemplu, certificatul digital ale Autorității de Certificare - DigiSign Qualified Public CA v2, nu poate fi utilizat pentru alte funcții decât cele specifice unei AC. Mai mult, certificatele digitale emise pentru Abonați nu pot fi utilizate ca certificate digitale de autentificare a serverelor WEB sau pentru emiterea unor alte certificate.

4. Tarife

Serviciile de certificare sunt oferite la tarifele stabilite de către DigiSign în funcție de natura și complexitatea serviciului solicitat și sunt publicate pe site-ul propriu, la adresa: https://www.digisign.ro/.

DigiSign își rezervă dreptul de a percepe tarife suplimentare pentru orice serviciu adițional, precum: servicii de implementare, instruire, consultanță etc, dacă acestea fac obiectul acordului între părți.

Serviciile de certificare furnizate de către DigiSign pot fi achitate prin diferite modalități de plată: numerar, ordin de plată sau carduri bancare, în baza unei facturi, conform reglementărilor legale în vigoare.

5. Actualizări

Modificările care pot surveni în conținutul acestui document sunt determinate de schimbări apărute în contextul legal, economic sau social, privind semnătura electronică, dar pot apărea și în urma unor acțiuni întreprinse de DigiSign cu scopul de a îmbunătăți periodic fluxurile operaționale.

DigiSign își rezervă toate drepturile de a efectua modificări de formă sau conținut asupra prezentului document. Cu ocazia efectuării unor modificări, departamentul responsabil actualizează implicit numărul versiunii pentru prezent document, cât și al Codului de Practici și Proceduri DigiSign, precum și data de emitere a acestora, în funcție de data la care au fost efectuate respectivele modificări.

Orice revizuire a Politicii de Certificare, fără impact sau cu un impact nesemnificativ asupra utilizatorilor – Abonați sau Entități Partenere, se poate realiza fără o notificare a acestora și nu implică modificarea numărului versiunii sau data de intrare în vigoare a prezentului document.

Prezentul document reprezintă Politica de Certificare DigiSign și este datat în 10.08.2015, fiind disponibil astfel:

- în format electronic, la adresa: https://www.digisign.ro/
- în format fizic, solicit printr-o scrisoare trimisă către sediul social DigiSign.

Politica de Certificare DigiSign este considerată validă și intră în vigoare din momentul publicării acesteia pe site-ul DigiSign.

Nr. Crt.	Versiune	Data publicării	Denumire
1	1.0	10.08.2015	Politica de Certificare DigiSign