PKI Disclosure Statement

Autoritatea de Certificare DigiSign

Certificate digitale calificate

conform Regulamentului eIDAS și legislației naționale

Categorie:	**Document Public**	Limba:	**Română**
Emis de:	**Organismul de Gestionare a Politicilor DigiSign**		
Verificat de:	**Auditor Intern**	Ediția:	**1**
Aprobat de:	**General Manager**	Verisunea:	**2.1**

OID: **1.3.6.1.4.1.34285.5.1.1.3.1.1.0**

DIGISIGN S.A.

Str. Virgil Madgearu, nr. 2 – 6, sector 1

014135, București, România

+4 031 620 20 00

+4 031 620 20 80

office@digisign.ro

www.digisign.ro

Copyright © DigiSign. Toate drepturile rezervate. Acest document nu va fi duplicat, utilizate, reprodus, publicat sau diseminat, în întreg sau în parte, pentru nici un scop, fără aprovarea prealabilă a DigiSign.

Istoric document

Ediție	Versiune	Descriere	Data	Emitent
1	1	Prima redactare: PKI Disclosure Statement – limba română	15 mai 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign
1	2	Actualizări aduse ca urmare a auditului	15 iunie 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign
1	2.1	Actualizări date de contact și metode de identificare	22 Noiembrie 2018	Organismul de Gestionare al Politicilor din cadrul DigiSign

Cuprins

1. Introducere

Acest document se numește PKI Disclosure Statement al Autorității de Certificare DigiSign (denumit în continuare PDS), fiind redactat în conformitate cu modelul prezentat în Anexa A a standardului ETSI EN 319 411-1. Acest document reprezintă un instrument suplimentar și simplificat care vine în sprijinul utilizatorilor de servicii de încredere calificate furnizate de DigiSign pentru înțelegerea corespunzătoare a condițiilor de furnizare a acestor servicii.

1.1. Scop

PDS conține referințe despre certificatele digitale calificate emise de CA DigiSign în calitate de prestator de servicii de încredere calificate, în conformitate cu Regulamentul UE nr. 910/2014 (în continuare denumit Regulamentul eIDAS), legislația națională aplicabilă și standardele relevante în domeniu.

1.2. Coordonate de contact

Nume	**DIGISIGN S.A.**
Adresă	**Str. Virgil Madgearu, nr. 2 – 6, Sector 1, București, România**
CUI	**RO 175544945**
Telefon	**+4 031 620 20 00**
Fax	**+4 031 620 20 00**
E-mail	**office@digisign.ro**
Website	**www.digisign.ro**
Program cu publicul	**Luni – Vineri, între 09:00 și 17:00**

2. Tipuri de certificate, proceduri și utilizare

DigiSign emite certificate digitale calificate pentru utilizatorii finali prin intermediul unor profile predefinite în cadrul Autorității de Certificare Intermediară DigiSign Qualified Class 3 CA 2017, emisă și semnată de către Autoritatea de Certificare Rădăcină DigiSign Root Certification Authority, în conformitate cu profilele descrise în standardul ETSI EN 319 412 Partea 1, 2, 3 și 5.

2.1. Certificat digital calificat pentru semnătura electronică

Informații generale
▪ Este emis în numele unei persoane fizice ▪ Poate conține un pseudonim, caz în care acest lucru va fi clar indicat ▪ Poate conține atribute referitoare la organizația, departamentul și funcția deținută de persoana fizică în cadrul unei organizații, în cazul în care reprezentantul legal al respectivei organizații autorizează introducerea acestor atribute în certificat
Politica de Certificare
▪ Emis de DigiSign Qualified Class 3 CA 2017 în QSCD ▪ OID: 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017 ▪ Tipul politicii de certificare: NCP+ ▪ QC Statement: qc-n / qc-n-qscd / qc-n-qscd-r
Identificare și autentificare
Scopul unui certificat digital calificat pentru semnături electronice este de a identifica subiectul acestuia cu un nivel ridicat de încredere și de a crea semnături electronice calificate, în conformitate cu Regulamentul UE nr. 910/2014 și legislația națională aplicabilă. În acest sens, identificarea unui solicitant se realizează după cum urmează: ▪ Identificarea solicitantului față-în-față, în baza unui act de identitate valid în original, de către o Autoritate de Înregistrare din cadrul DigiSign ▪ Identificarea solicitantului de către un notar public autorizat ▪ Identificarea solicitantului prin intermediul unui certificat digital calificat emis de Autoritatea de Certificare DigiSign ▪ Identificarea solicitantului prin metode de identificare ce oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică.
Procesul de înregistrare
Solicitantul completează formularul de înregistrare aferent obținerii unui certificat digital calificat pentru semnătură electronică, disponibil la adresa www.digisign.ro. Solicitantul prezintă Autorității de Înregistrare documentele necesare procesului de emitere și actul de identitate valid în original. Operatorul Autorității de Înregistrare verifică actul de identitate prezentat de solicitant în original în ceea ce privește valabilitatea, integritatea și existența elementelor de securiate ale actului, precum și asocierea dintre act și solicitant. Solicitantul poate trimite documentația necesara procesului de emitere și prin servicii poștale sau de curierat sub condiția ca acestea să fie autentificate în prealabil de către un notar public autorizat. Solicitantul se obligă să prezinte Autorității de Înregistrare următoarele: ▪ Documente valide de identificare care confirmă identitatea acestuia ▪ Contractul de prestări servicii de încredere, datat și semnat ▪ Condițiile generale de furnizare a serviciilor de încredere, datate și semnate ▪ Declarație, semnată și datată În cazul în care solicitantul dorește includerea în certificat a informațiilor referitoare la legătura dintre acesta și o persoana juridică, precum denumirea persoanei juridice și departamentul și funcția pe care o deține, atunci solicitantul trebuie să facă dovadă acestei legături prin prezentarea unor documente oficiale în acest sens.
Utilizare permisă
▪ Crearea și validarea semnăturilor electronice ▪ Autentificare

Limite și utilizări interzise
▪ Criptare ▪ Key Escrow

2.2. Certificat digital calificat pentru sigiliul electronic

Informații generale
▪ Este emis în numele unei persoane juridice
Politica de Certificare
▪ Emis de DigiSign Qualified Class 3 CA 2017 în QSCD ▪ OID: 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017 ▪ Tipul politicii de certificare: NCP+ ▪ QC Statement: qc-l / qc-l-qscd / qc-l-qscd-r
Identificare și autentificare
Scopul unui certificat digital calificat pentru sigilii eletronice este de a identifica subiectul acestuia cu un nivel ridicat de încredere și de a crea sigilii electronice calificate, în conformitate cu Regulamentul UE nr. 910/2014. În acest sens, identificarea persoanei juridice se realizează după cum urmează, prin reprezentatul autorizat al acesteia care întotdeauna este o persoană fizică: ▪ Identificarea solicitantului față-în-față, în baza unui act de identitate valid în original, de către o Autoritate de Înregistrare din cadrul DigiSign ▪ Identificarea solicitantului de către un notar public autorizat ▪ Identificarea solicitantului prin intermediul unui certificat digital calificat emis de Autoritatea de Certificare DigiSign ▪ Identificarea solicitantului prin metode de identificare ce oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică.
Procesul de înregistrare
Solicitantul completează formularul de înregistrare aferent obținerii unui certificat digital calificat pentru sigiliul electronic, disponibil la adresa www.digisign.ro. Solicitantul prezintă Autorității de Înregistrare documentele necesare procesului de emitere și actul de identitate valid în original. Operatorul Autorității de Înregistrare verifică actul de identitate prezentat de solicitant în original în ceea ce privește valabilitatea, integritatea și existența elementelor de securiate ale actului, precum și asocierea dintre act și solicitant. Solicitantul poate trimite documentația necesara procesului de emitere și prin servicii poștale sau de curierat sub condiția ca acestea să fie autentificate în prealabil de către un notar public autorizat. Solicitantul se obligă să prezinte Autorității de Înregistrare următoarele: ▪ Documente valide de identificare care confirmă identitatea acestuia ▪ Contractul de prestări servicii de încredere, datat și semnat ▪ Condițiile generale de furnizare a serviciilor de încredere, datate și semnate ▪ Declarație, semnată și datată ▪ Certificat constatator, valid, din care rezultă reprezentantul legal al persoanei juridice, sau echivalentul acestui document în cazul persoanelor juridice străine ▪ Împuternicire oficială în cazul în care solicitantul nu este reprezentantul legal al persoanei juridice, care să demonstreze autorizarea acestuia de către reprezentnatul legal al persoanei juridice.
Utilizare permisă
▪ Crearea și validarea sigiliilor electronice ▪ Autentificare
Limite și utilizări interzise

- Criptare
- Key Escrow

3. Răspundere financiară

DigiSign va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfășurării activității de certificare, tuturor persoanelor care își întemeiază conduita pe efectele juridice ale certificatelor digitale calificate, până la concurența echivalentului în lei (RON) a sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat reprezintă fiecare prejudiciu produs, chiar dacă se produc mai multe asemenea prejudicii ca urmare a neîndeplinirii de către furnizor a unei obligații prevăzute de lege.

4. Obligațiile utilizatorilor

Utilizatorii au obligația de a respecta prevederile Politicilor de Certificare și ale Codurilor de Practici și Proceduri aplicabile. Obligațiile principale ale acestora sunt:

- Familiarizarea acestora cu politicile de certificare sub care sunt emise certificatele digitale calificate solicitate, pentru a putea înțelege obligațiile ce îi revin
- Furnizarea informațiilor reale și complete atunci când se înregistrează
- Respectarea obligațiilor asumate prin semnarea condițiilor generale de furnizare a serviciilor de încredere și a acordurilor aferente
- Verificarea datelor introduse în cererile de înregistrare și în certificatele digitale emise în sensul acureteții acestora cu datele furnizate
- Utilizarea dispozitivelor criptografice securizate și cheilor private stocate în acestea de așa manieră încât să prevină accesul neautorizat, precum și exercitarea controlului asupra cheii private doar de către el însuși
- Utilizarea certificatelor digitale calificate doar în scopurile pentru care acestea au fost emise și conform politicilor de certificare ale acestora
- Notificarea de îndată a DigiSign în cazul compromiterii cheilor private, în sensul solicitării revocării certificatului digital calificat.

5. Obligațiile Entităților Partenere

O Entitate Parteneră poate fi orice entitate care acceptă o semnătură electronică calificată, un sigilu electronic calificat sau o marcă temporală calificată creată cu un certificat digital caificat emis de DigiSign și care se bazează pe:

- Validitatea conexiunii dintre certificat și identitatea titularului acestuia
- Validitatea confirmării emise de serviciul de validare a certificatelor digitale furnizat de DigiSign.

Obligațiile generale ale unei Enități Partenere sunt:

- Verificarea semnăturii/sigiliului/mărcii temporale create cu un certificat digital calificat emis de DigiSign

- Verificarea documentului semnat/sigiliat/marcat temporal în sensul nealterării acestuia după aplicarea semnăturii/sigiliului/mării temporale
- Utilizarea corespunzătoare a operațiilor criptografice, utilizând aplicații software și dispozitive care asigură un nivel de încredere corespunzător celui necear
- Refuzarea unei semnături/sigiliu/marcă temporală sau a certificatului aferent în cazul în care în urma verificării acestora rezultatul este unul negativ, însă nu înainte de a se asigură ca mijloacele și instrumentele de verificare au fost utilizate corespunzător
- Acceptarea și încrederea doar în acele certificate digitale calificate care sunt utilizate în conformitate cu scopul declarat al acestora.

6. Limitări

În limitele stabilite de legislația națională aplicabilă, cu excepția fraudei sau a abaterilor intenționate, DigiSign nu va fi responsabilă pentru orice pierdere a profitului, a datelor sau orice daune indirecte, consecvente sau punitive, rezultate din sau în legătură cu utilizarea serviciilor de încredere furnizate.

7. Alte aspecte

Toate informațiile referitoare la certificatele digitale calificate emise de DigiSign sunt puse la dispoziția publicului la adresa www.digisign.ro, iar orice parte interesată în a le accesa nu are nevoie de credențiale de acces în acest sens.

Documentele care guvernează certificatele digitale calificate emise de DigiSign sunt:

- Policita de Certificare a Autorității de Certificare DigiSign
- Codul de Practici și Proceduri al Autorității de Certificare DigiSign
- PKI Disclosure Statement
- Politica și Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign

8. Politica de Confidențialiate

Toate informațiile cu caracter confidențial sunt colectate, stocate și prelucrate de către DigiSign în conformitate cu prevederile legale aplicabile în ceea ce privește prelucrare datelor cu caracter personal și protecția acestora. Mai multe detalii în acest sens se găsesc în Codul de Practici și Proceduri al Autorității de Certificare DigiSign.

9. Politica de restituire

DigiSign oferă posibilitatea restituire tarifelor achitate către utilizatori, în conformitate cu Politica de Restituire publicată la adresa www.digisign.ro. Utilizatorii care invocă această

politică trebuie să aibă toate certificatele revocate și să demonstreze nerespectarea obligațiilor de către DigiSign, specificate în acordul semnat între cele două părți.

10. Legea aplicabilă, plângeri și rezolvarea disputelor

Acest document se bazează pe regulile generale descrise în Codul de Practici și Proceduri al Autorității de Certificare DigiSign, în conformitate cu prevederile legale naționale aplicabile, precum și cu prevederile legale europene. Eventualele dispute privind serviciile de încredere calificate furnizate de DigiSign, se vor rezolva pe cale amiabilă. Dacă disputa nu este rezolvată pe cale amiabilă în decurs de 30 de zile, părțile se pot adresa instanțelor judecătorești competente din București. În cazul existenței unei plângeri privind serviciile furnizate de către DigiSign, utilizatorii se obligă întâi să notiifce DigiSign în acest sens.

11. Autoritatea de Certificare, depozitarul, marca de încredere și audit

DigiSign are calitatea de prestator de servicii de încredere calificate, cu sediul în România. Furnizarea serviciilor de încredere calificate de către DigiSign, face subiectul unor evaluări și audituri de conformitate impuse de legislația europeană și națională aplicabilă.

DigiSign deține următoarele certificări:

- ISO 27001:2013 care certifică faptul că DigiSign a implementat un Sistem de Management Integrat care respectă cerințele acestui standard în ceea ce privește serviciile pe care le furnizează
- ISO 18001:2007 care certifică faptul că DigiSign îndeplinește cerințele acestui standard în ceea ce privește serviciile pe care le furnizează
- ISO 14001:2004 care certifică faptul că DigiSign îndeplinește cerințele acestui standard în ceea ce privește serviciile pe care le furnizează
- ISO 9001:2008 care certifică faptul că DigiSign îndeplinește cerințele acestui standard în ceea ce privește serviciile pe care le furnizează
- Aprobare și includere în registrul național de evidență al operatorilor autorizați de prelucare a datelor cu caracter personal, administrat de ANPDSC
- ETSI EN 319 401, EN 319 411, EN 319 412, EN 319 421 și EN 319 422 care certifică faptul că DigiSign furnizează servicii de încredere calificate conform Regulamentului nr. 910/2014 (eIDAS).

În calitate de prestator de servicii de încredere calificat, în conformitate cu Regulamentul eIDAS, DigiSign are dreptul de a afișa Marca Europeană de Încredere.

Depozitarul DigiSign este disponibil oricărei părți interesate la adresa www.digisign.ro.