Politica de Certificare

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**

OID: **1.3.6.1.4.1.34285.1.1.1.1.2.1.0**

Status: ***Spre abrobarea Organismului de Supraveghere***

DIGISIGN S.A.

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

014135, București, România

+4 031 620 12 89

+4 031 620 20 99

office@digisign.ro

www.digisign.ro

Istoria documentului

Ediție	Versiune	Descriere	Data	Emitent
1	1	Prima redactare: Politica de Certificare a Autorității de Certificare DigiSign, în conformitate cu Regulamentul eIDAS și legislația națională aplicabilă	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

Cuprins

1. Introducere

Politica de Certificare (denumită în continuare CP) reprezintă un set anume de reguli și principii sub care sunt emise tipuri de certificate digitale aparținând unei comunități anume și/sau unei clase de aplicații cu aceleași cerințe de securitate.

Scopul Politicii de Certificare este de a stabili, în termeni generali, ce anume trebuie să facă un participant al DigiSign PKI, precum și aria de aplicabilitate a unui certificat în conformitate cu tipul/clasa acestuia. Regulile și principiile stabilite în acest document determină nivelul de securitate și asigurare al unui anumit tip de certificate.

1.1. Prezentare generală

DIGISIGN S.A. (denumită în continuare DigiSign) operează o infrastructură de chei publice (denumită în continuare PKI) în vederea furnizării de servicii de încredere, precum: semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate. DigiSign PKI utilizează o Autoritatea de Certificare cu rol de rădăcină, sub care sunt emise Autorități de Certificare intermediare dedicate unei clase sau unui anumit tip de serviciu. În cadrul unei Autorități de Certificare Intermediară sunt definite mai multe profile de certificate pentru a emite un tip de certificat specific unei anumite clase sau aplicabilități.

În calitate de Autoritate de Certificare (denumită în continuare CA), DigiSign emite certificate digitale atât entităților din cadrul sectorului public, cât și celui privat, dar și persoanelor fizice, în conformitate cu regulile, principiile și practicile defințe în acest document. În rolul său de CA, DigiSign operează funcții asociate cu operații criptografice care includ, dar nu se limitează la, cereri, emitere, revocare, suspendare, reînnoire de certificate digitale, emiterea și publicarea Listelor de Certificate Revocate (denumite în continuare CRL), precum și menținerea unui serviciu de verificare în timp real al certificatelor, bazat pe protocolul Online Certificate Status Protocol (denumit în continuare OCSP).

DigiSign este unul din principalii Prestatori de Servicii de Încredere Calificate care reușește cu succes să furnizeze servicii de încredere precum semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate, având în același timp și un rol de Terță Parte de Încredere (denumită în continuare TTP) în ceea ce privește crearea și validarea serviciilor respective.

Acest document descrie regulile generale și principiile implementate de DigiSign în calitate de prestator de servicii de încredere calificate, în vederea emiterii, reînniorii, suspendării, revocării, validării și, în generale, a administării certificatelor digitale emise, în conformitate cu cerințele legale aplicabile în materie, respectiv:

- ✓ Regulamentul UE nr. 910/2014 (denumit în continuare Regulamentul eIDAS) privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice și de abrogare a Directivei 1999/93/EC, precum și a regulamentelor și directivelor subsecvente acestuia
- ✓ Legislația națională aplicabilă, în vigoare

1.2. Participanți din cadrul DigiSign PKI

Participanți ai DigiSign PKI sunt acele entități care îndeplinesc un rol în DigiSign PKI fie prin utilizarea și prin furnizarea serviciilor de certificare. Astfel sunt identificați următorii participanți:

- Autoritățile de Certificare (CA)
- Autoritățile de Înregistrare (RA)
- Autoritățile de Validare (VA)
- Beneficiarii (Subscribers)
- Titularii (Subjects)
- Terțe părți interesate (Relying Parties)
- Alți participanți: Autoritățile de Marcare Temporală (TSA), depozitarul DigiSign etc

În timp ce o Autoritate de Certificare are rolul de a asigura administrarea corespunzătoare a certificatelor digitale emise și, în unele cazuri, poartă responsabilitatea întregului proces, Utilizatorii – reprezentați de Titulari, Beneficiari și Entități Partenere – au responsabiliatea de a utiliza un certificat digital calificat în conformitate cu politica acestuia. Politica și scopul unui certificat au de asemenea un impact major asupra Entităților Partenere datorită responsabilității acestora de a decide dacă certificatul respectiv corespunde nivelul de asigurare necesar.

DigiSign emite certificate digitale oricărui solicitant, în limita prevederilor legale, și atât timp cât aceștia sunt de acord și respectă Politica de Certificare și Codul de Practici și Proceduri.

Titularul unui certificat digital este reprezentat de către entitatea înscrisă în câmpul *Subject* din structura certificatului și care nu emite certificate către alte entități, în cazul certificatelor emise către utilizatorii finali. Titularul unui certificat digital emis de CA DigiSign poate fi:

- o persoană fizică
- o persoană fizică identificată în asociație cu o persoană juridică (certificatul conține atribute specifice privind persoana juridică care este legată de persoana fizică)
- o persoană juridică

De asemenea, Autoritățile de Certificare și de Marcare Temporală din cadrul DigiSign pot fi titulari de certificate digitale

Beneficiarii sunt reprezentați de către entitățile care înaintează o solicitare către DigiSign în vederea obținerii unuia sau mai multor certificate digitale. În general, Beneficiarul este Titular certificatului însuși, însă sunt cazuri în care Beneficiarul acționează în numele unuia sau a mai multor Titulari distincți, de care este legat (exemplu: Beneficiarul este o companie care solicita certificate pentru angajații săi în vederea participării la tranzacții electronice în numele și pentru companie). Astfel, având în vedere tipul de certificat solicitat Beneficiarul poate fi:

a. în cazul unui certificat digital calificat pentru semnătură electronică
- persoana fizică însuși, titular al certificatului digital
- persoana fizică mandatată de către titular
- persoana juridică de care este legată persoana fizică, titular al certificatului

b. în cazul unui certificat digital calificat pentru sigiliu electronic
- persoana fizică, reprezentant legal al persoanei juridice
- persoana fizică, reprezentant autorizat/împuternicit/mandatat de către reprezentantul legal al persoanei juridice

O entitate parteneră poate fi reprezentată de o persoană sau de un dispozitiv, care se bazează pe un certificat digital emis de DigiSign sau pe o operațiune criptografică realizată cu un certificat digital emis de DigiSign.

Toți participanții din cadrul DigiSign PKI sunt prezentați și descriși în termeni legali, comerciali și tehnici, în Codul de Practici și Proceduri al Autorității de Certificare DigiSign.

1.3. Identificarea documentului

Numele acestui document este Politica de Certificare a Autorității de Certificare DigiSign (denumită în continuare CP) și descrie regulile și principiile aplicabile unui anumit tip de certificat emis de Autoritățile de Certificare din cadrul DigiSign. CP este aplicabil tuturor participanților din cadrul DigiSign PKI care utilizează serviciile de încredere furnizate.

CP descrie în termeni generali, regulile și principiile implementate în vederea asigurării conformității cu Regulamentul UE nr. 910/2014 (denumit în continure Regulamentul eIDAS) și legislația națională aplicabilă, în ceea ce privește furnizarea de servicii de încredere calificate, precum semnăturile electronice calificate, sigiile electronice calificate și mărcile temporale calificate. Descrierea completă și detaliată a acestor servicii se găsește în Codul de Practici și Proceduri al Autorității de Certificare DigiSign.

2. Tipuri de certificate

Un certificat electronic (sau digital) reprezintă o suită de informații și atribute care leagă datele de semnare cu datele de verificare de o entitate și care confirma identitatea acesteia.

Un certificat pentru semnătură electronică înseamnă o atestare electronică care face legătura între datele de validare a semnăturii electronice și o persoană fizică și care confirmă cel puțin numele sau pseudonimul persoanei respective. Un certificat calificat pentru semnătură electronică înseamnă un certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa I a Regulamentului eIDAS.

Un certificat pentru sigiliul electronic înseamnă o atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă numele persoanei respective. Un certificat calificat pentru sigiliul electronic înseamnă un certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa III din Regulamentul eIDAS.

Astfel, DigiSign în calitate de prestator de servicii de încredere calificat, emite următoarele tipuri de certificate persoanelor fizice și persoanelor juridice, având un nivel ridicat de asigurare.

Autoritate de Certificare	Tip	Subiect	QC Statement	Nivel de încredere	Garanții și răspundere financiară
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017					
DigiSign Qualified CA Class 3 2017	Certificat electronic calificat	Persoana fizică	qc-n	Ridicat	Complet
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017					

DigiSign Qualified CA Class 3 2017	Certificat electronic calificat cu pseudonim	Persoana fizică	qc-n	Ridicat	Complet
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017					
DigiSign Qualified CA Class 3 2017	Certificat electronic calificat emis pe QSCD	Persoana fizică	qc-n-qscd	Ridicat	Complet
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017					
DigiSign Qualified CA Class 3 2017	Certificat electronic calificat cu pseudonim emis pe QSCD	Persoana fizică	qc-n-qscd	Ridicat	Complet
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017					
DigiSign Qualified CA Class 3 2017	Certificat electronic calificat	Persoană juridică	qc-l	Ridicat	Complet
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.2.3.042017					
DigiSign Qualified CA Class 3 2017	Certificat electronic calificat emis pe QSCD	Persoană juridică	qc-l-qscd	Ridicat	Complet
Policy identifier (OID number): 1.3.6.1.4.1.34285.1.2.4.256.2.1.3.042017					
DigiSign Qualified CA Class 3 2017	Certificat electronic calificat pentru CA	Autorități din cadrul DigiSign PKI		Ridicat	Complet

Certificatele digitale emise de Autoritatea de Certificare DigiSign Qualified CA Class 3 2017 sunt certificate digitale calificate care asigură un nivel ridicat de încredere. Certificatele digitale calificate au scopul de a crea și verificarea semnături electronice, sigilii electronice și mărci temporale, în conformitate cu Regulamentul eIDAS și legea națională aplicabilă. Certificatele digitale calificate emise de DigiSign determină cu un nivel de precizie înalt identitatea titularului, autenticitatea unei organizații sau credibilitatea unei Autorități.

Astfel, procesul de înregistrare pentru un certificat digital calificat se realizează prin completarea unui formular aferent care necesită specificarea unor informații complete și corecte în ceea ce privește identitatea solicitantului. În afara de verificarea domeniului de care aparține adresa de e-mail furnizata de solicitant, Autoritatea de Înregistrare (denumită în continuare RA) verifică documentele înaintate de către solicitant în sensul validării acestora și a clasificării lor ca și corespunzătoare sau nu, după caz. Pentru certificatele digitale calificate, documentele de identificare ale solicitantului, acceptate sunt cele stabilite de legislația națională aplicabilă și pot fi: act de identitate, pașaport, carte de rezident, certificat de înregistrare fiscală (spre exemplu, certificatul de naștere nu este

considerat un document de identitate acceptat). Toate informațiile solicitate de la și furnizate de către solicitant fac obiectul unei verificări riguroase de către RA din domeniul DigiSign, în ceea ce privește certificatele digitale calificate.

Mai mult, pentru certificatele digitale calificate, solicitanților le este impus să se prezinte personal la una din RA din domeniul DigiSign, conform prevederile CPP și a procedurilor publicate la adresa www.digisign.ro, în vederea identificării corespunzătoare a acestuia, în baza unui act de identitate valid, în original.

Certificatele digitale calificate pentru semnătură electronică emise de CA DigiSign pot fi utilizate pentru crearea și validarea semnăturilor electronice, care beneficiază de același efect legal ca și semnăturile olografe. Certificatul digital calificat asigură identitatea titularului acestuia și non repudierea documentului semnat.

Certificatele digitale calificate emise de DigiSign Qualified CA Class 3 2017 pentru alte autorități din cadrul domeniului DigiSign au ca scop principal Autăritățile de Validare și Autoritățile de Marcare Temporală.

Pentru certificatele digitale calificate, DigiSign asigură garanția completă a răspunderii, conform prevederilor CPP.

3. Servicii

DigiSign în calitate de prestator de servicii de încredere calificate, asigură următoarele servicii: înregistrarea, verificarea, emiterea, reînnoirea, publicarea, suspendarea, revocarea, administrarea și depozitarea certificatelor digitale emise, precum și servicii de marcare temporală, implementare și școlarizare de soluții bazate pe infrastructuri de chei publice.

Serviciile de încredere furnizate de DigiSign au propriile reguli și proceduri, în conformitate cu prevederile CPP, fiind sumarizate în prezentul document după cum urmează:

a. Înregistrarea: presupunde înregistrarea unui solicitant și implica verificarea și autentificarea cererii și identității acestuia.

b. Emiterea: presupune emiterea unui certificat digital de către CA din domeniul DigiSign, dacă procesul de înregistrare a fost închis cu succes

c. Reînnoirea: presupune emiterea unui nou certificat digital calificat de către aceeași CA din domeniul DigiSign care a emis certificatul inițial, aceluiași titular, sub condiția ca acesta să inițieze procesul de reînnoire. Depinzând de metoda de reînnoire, anumite informații despre solicitant pot fi schimbate (spre exemplu, adresa, numărul de telefon etc)

d. Publicarea: presupune publicarea și depozitarea unui certificat digital emis, acțiune ce se realizează întotdeaună după acceptul titularului; depozitarea se realizează în registrul electronic de evidență a certificatelor emise de DigiSign și este permanent accesibil publicului la adresa www.digisign.ro, aceasta fiind și sursa principală de informare și comunicare cu participanții din cadrul DigiSign PKI

e. Suspendarea: presupune revocarea temporară și reversibilă a unui certificat digital

f. Revocarea: presupune anularea definitivă a validității unui certificat digital și retragerea oricărui drept de utilizare a acestuia

g. Validarea: presupune verificarea certificatului digital în timp real prin serviciului OCSP, ori verificarea certificatului digital prin consultarea Listelor de Certificate Revocate (acest serviciu oferă o dată la 24 de ore informații privind statusul unui certificat, în special dacă acesta a fost revocat sau nu), ori verificarea certificatului digital prin consultarea registrului electronic de evidență a certificatelor emise

h. Marcare Temporală: reprezintă un serviciu adițional oferit de Autoritatea de Marcare Temporală DigiSign, descris în propriul CPP și care presupune confirmarea existenței unui informații electronice într-un anumit format la un moment de timp dat.

4. Tarife

Serviciile de încredere furnizate de DigiSign sunt disponibile public din punct de vedere comercial. Tarifele pentru aceste servicii depind în funcție de natura și complexitatea seriviciului solicitat. Tarifele pentru fiecare serviciu este publicat la adresa www.digisign.ro.

DigiSign își rezervă dreptul de a aplica tarife suplimentare pentru serviciile adiționale furnizate, precum implementare, instruire, consultanță etc, sub condiția încheierii unui acord cu solicitantul în acest sens.

5. Amendamente

Policita de Certificare DigiSign este administrată de către Organismul de Gestionare a Politicilor din cadrul DigiSign, în conformitate cu cap. 1.4 al Codului de Practici și Proceduri al Autorității de Certificare DigiSign.

6. Alte informații

Politica de Confidențialitate

DigiSign a implementat o politică de confidențialitate în conformitate cu CPP. Politica de confidențialitate este disponibilă public și poate fi consultată la adresa www.digisign.ro.

Publicare și comunicare

Serviciile de încredere furnizate de DigiSign și conținutul depozitarului, pot fi accesate prin diferite mijloace de comunicare, precum:

- Prin web: www.digisign.ro
- Prin e-mail: office@digisign.ro
- Fizic: str. Virgil Madgearu, nr. 2 – 6, sector 1, București, 014135, România

În general, websiteul oficial al DigiSign – www.digisign.ro – va fi utilizat pentru orice comunicare și notificare către utilizatorii serviciilor de încredere oferite de DigiSign. Alte metode de comunicare și notificare individuală sunt specificate în CPP.

Disponibilitate

DigiSign asigură programul cu publicul de luni până vineri, între orele 09:00 și 17:00, cu excepția sărbătorilor legale naționale și pune la dispozitia Utilizatorilor și oricăror alte părti interesate, departamentul HelpDesk 24 de ore din 24, 7 zile din 7, la numărul de telefon 031 620 12 89 sau prin e-mail la helpdesk@digisign.ro, privind orice informații referitoare la serviciile de încredere calificate furnizate, precum și alte produse și servicii conexe.

DigiSign garantează accesul la sediul din str. Virgil Madgearu, nr. 2 – 6, sector 1, București, România, persoanelor cu dizabilități prin asgiurarea unui loc de parcare special amenajat, a unei rampe de acces și a liftului care dispune de indicații sonore și vizuale. Mai mult, DigiSign asigură instrumente de tip "mărire" și ajustare a contrastului pentru website-ul www.digisign.ro.