Declarația de informare a PKI (PDS)

CertDigital

EMISĂ DE:			
DEPARTAMENT	**NUME**	**SEMNĂTURA**	**DATA**
MANAGEMENTUL POLITICILOR ȘI PROCEDURILOR	Ofițer de Securitate IT		_____

APROBATĂ DE:			
DEPARTAMENT	**NUME**	**SEMNĂTURA**	**DATA**
MANAGEMENTUL POLITICILOR ȘI PROCEDURILOR	Director General		_____

ISTORICUL MODIFICĂRILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICĂRI**	**DATA:**
1.0–1.6	—	Declarația de informare a PKI pentru generațiile G2, G3 și G4 (30.04.2017 – 01.11.2025; versiunea 1.6: serviciul QPS)	01/11/2025
2.0	Ofițer de Securitate IT	Rescriere după ETSI EN 319 411-1, anexa A: generațiile G4 și G5 (certificatele titularilor și certificatele de serviciu ale CERTDIGITAL QCA G5), adresele fixe la care trimite declarația QcPDS (ro, en), Legea nr. 214/2024; G2 expirată, G3 retrasă; înlocuiește versiunea 1.6	23/10/2026
2.1	Ofițer de Securitate IT	Atestarea de conformitate se publică la https://www.certdigital.ro/repository/conformitate/ după emitere, alături de deciziile ADR privind statutul calificat; legătura ANPC pentru SAL devine https://anpc.ro/sal; trimiterile la documentele asociate, la versiunile în vigoare (PDP-rQSCD v2.1, TC-CERT v2.1, TC-rQSCD v1.2); cuprinsul începe pe pagină nouă	27/10/2026
2.2	Ofițer de Securitate IT	Trimiterile la celelalte documente CertDigital nu mai au număr de versiune: se aplică versiunea în vigoare, publicată la adresa fixă din depozit, iar versiunile anterioare sunt în arhivă; lista documentelor aplicabile înlocuiește tabelul cu versiuni	27/10/2026
2.3	Ofițer de Securitate IT	Certificatele de scurtă durată ale cheilor de unică folosință din serviciul rQSCD: identificatorul 1.3.6.1.4.1.47898.11.1.2, valabilitatea de cel mult 60 de minute, verificarea identității, revocarea și starea după expirare (secțiunile 2.2 și 2.4)	02/11/2026

Cuprins

1. Documentul și datele de contact 5
1.1. Natura documentului 5
1.2. Prestatorul și datele de contact 5
1.3. Cererea de revocare 6
2. Tipurile de certificate, verificarea identității și utilizarea 7
2.1. Ierarhiile de certificare 7
2.2. Certificatele titularilor 7
2.3. Verificarea identității 8
2.4. Certificatele pentru chei gestionate în QSCD la distanță 8
2.5. Certificatele de serviciu ale CERTDIGITAL 9
2.6. Utilizarea, reînnoirea și revocarea 10
3. Limitele de încredere 11
4. Obligațiile titularului și ale abonatului 12
5. Obligațiile părților care se bazează 13
6. Garanția limitată și limitarea răspunderii 14
7. Documentele aplicabile 15
8. Protecția datelor cu caracter personal 16
9. Tarifele și rambursarea 17
10. Legea aplicabilă, reclamațiile și soluționarea litigiilor 18
11. Statutul calificat, evaluarea conformității și auditul 19

1. Documentul și datele de contact

1.1. Natura documentului

Prezentul document este declarația de informare privind infrastructura de chei publice (PKI Disclosure Statement – PDS) a CENTRUL DE CALCUL S.A. (marca CertDigital, denumit în continuare „CERTDIGITAL"), întocmită după modelul din ETSI EN 319 411-1, anexa A. El rezumă, pentru titulari, abonați și părțile care se bazează, condițiile principale în care CERTDIGITAL emite și gestionează certificatele calificate pentru semnătura electronică și pentru sigiliul electronic ale generațiilor G4 și G5, precum și certificatele de serviciu ale CERTDIGITAL.

Documentul este un instrument simplificat de informare. El nu înlocuiește Politica serviciilor de certificare CertDigital, declarațiile practicilor de certificare (DPC CERTDIGITAL G4 și DPC CERTDIGITAL G5) și nici Termenii și condițiile pentru certificatele calificate (TC-CERT), care cuprind integral informațiile de mai jos și fac parte din contractul cu titularul (capitolul 7).

Declarația QcPDS (ETSI EN 319 412-5) din certificatele emise de CERTDIGITAL QCA G5 trimite la prezentul document, publicat la adrese fixe:

– în limba română: https://www.certdigital.ro/repository/pds/certdigital_pds_ro.pdf;

– în limba engleză: https://www.certdigital.ro/repository/pds/certdigital_pds_en.pdf.

În certificatele generației G4, declarația QcPDS trimite la pagina depozitului, https://www.certdigital.ro/repository, de unde este accesibil prezentul document. Versiunea în limba engleză are același conținut ca versiunea în limba română (ETSI EN 319 412-5, tabelul 2); în caz de neconcordanță, prevalează versiunea în limba română.

Versiunea 2.0 înlocuiește Declarația de informare a PKI, versiunea 1.6, care se păstrează în arhiva depozitului (https://www.certdigital.ro/repository/arhiva/).

1.2. Prestatorul și datele de contact

Element	Informație
Prestatorul de servicii de încredere calificat	CENTRUL DE CALCUL S.A. (marca CertDigital), Str. Tudor Vladimirescu nr. 17, Târgu Jiu, județul Gorj, cod poștal 210132, România; nr. de ordine în Registrul Comerțului J1991000103187; EUID ROONRC.J1991000103187; CUI RO2163993
Contact	tel. +40 253 214 767; e-mail office@certdigital.ro; https://www.certdigital.ro/; program cu publicul: luni–vineri, 09:00–17:00
Suport tehnic / vânzări	suport@certdigital.ro / sales@certdigital.ro
Protecția datelor (DPO)	dpo@centruldecalcul.ro
Depozitul de documente	https://www.certdigital.ro/repository/
Registrul certificatelor	https://ca.certdigital.ro/registry

Element	Informație
Certificatele autorităților	G4: adresele din DPC CERTDIGITAL G4, secțiunea 2.1; G5: http://certs.certdigital.ro/certdigital_root_g5.crt · http://certs.certdigital.ro/certdigital_qualified_g5.crt
Informații privind starea certificatelor	G4: OCSP http://ocsp.g4.certdigital.ro · CRL http://crl.certdigital.ro/certdigital_qualified_g4.crl; G5: OCSP http://ocsp.g5.certdigital.ro · CRL http://crl.certdigital.ro/certdigital_qualified_g5.crl
Organismul de supraveghere	Autoritatea pentru Digitalizarea României (ADR), www.adr.gov.ro

1.3. Cererea de revocare

Revocarea unui certificat se poate cere 24 de ore din 24, 7 zile din 7, prin portalul client https://ca.certdigital.ro/ra-web/apps/ota/, după autentificare. Cererea se poate transmite și prin e-mail semnat electronic calificat, la office@certdigital.ro, sau în scris, la sediu, în programul de lucru.

Pot cere revocarea titularul, abonatul care a obținut certificatul, reprezentantul legal al persoanei juridice titulare, instanța sau ADR; CERTDIGITAL poate revoca un certificat și din oficiu. Cererea se procesează în cel mult 24 de ore, iar revocarea este gratuită și definitivă (secțiunea 2.6).

2. Tipurile de certificate, verificarea identității și utilizarea

2.1. Ierarhiile de certificare

Generația	Autoritatea rădăcină	Autoritatea emitentă a certificatelor titularilor și a certificatelor de serviciu
G4	CERTDIGITAL ROOT CA G4	CERTDIGITAL QUALIFIED CA G4
G5	CERTDIGITAL ROOT CA G5 (RSA 4096, valabil 25 de ani)	CERTDIGITAL QCA G5 (RSA 4096, valabil 15 ani)

Autoritatea emitentă este indicată în fiecare certificat. Ierarhiile, certificatele autorităților și ale serviciilor și politicile sprijinite sunt descrise în documentul Ierarhia PKI CertDigital (IER-PKI).

Generația G3 (CertDigital ROOT CA G3 și autoritățile subordonate acesteia) nu mai emite certificate. Certificatele G3 emise rămân valabile până la expirare, cel târziu la 02.05.2027, în condițiile documentelor generației G3, păstrate în arhiva depozitului. Certificatele generației G2 au expirat.

2.2. Certificatele titularilor

Certificat	Politica ETSI (EN 319 411-2)	Identificatorul CERTDIGITAL	Efectul juridic
Certificat calificat pentru semnătura electronică (persoană fizică, inclusiv persoană fizică asociată unei persoane juridice)	QCP-n-qscd (0.4.0.194112.1.2)	1.3.6.1.4.1.47898.4.1.{1,2}.{1,4,6}.1 (G4); 1.3.6.1.4.1.47898.5.1.{1,2}.{1,4,6}.1 (G5)	Semnătura electronică calificată are efectul juridic echivalent al unei semnături olografe (art. 25 alin. (2) din Regulamentul eIDAS).
Certificat calificat pentru sigiliul electronic (persoană juridică)	QCP-l-qscd (0.4.0.194112.1.3)	1.3.6.1.4.1.47898.4.1.{1,2}.{1,4,6}.2 (G4); 1.3.6.1.4.1.47898.5.1.{1,2}.{1,4,6}.2 (G5)	Sigiliul electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii acestora (art. 35 alin. (2) din Regulamentul eIDAS).

Identificatorul CERTDIGITAL indică:

– dispozitivul (1 = tokenul titularului);

– generarea cheii (1 = de titular, prin aplicația CertDigital CSR; 2 = de CERTDIGITAL);

– metoda de verificare a identității (1 = prezență fizică; 4 = CERTDIGITAL KYC; 6 = certificat calificat CERTDIGITAL, la reînnoire);

– tipul titularului (1 = persoană fizică; 2 = persoană juridică).

Certificatele se emit publicului (persoane fizice și persoane juridice). Ele au o valabilitate de cel mult 3 ani (pentru certificatele de scurtă durată ale cheilor de unică folosință, secțiunea 2.4) și conțin declarațiile QcCompliance, QcSSCD, QcType și QcPDS (ETSI EN 319 412-5). Cheile titularilor

sunt RSA de 2048 de biți pentru certificatele emise până la 28.02.2027 și ECDSA pe curba NIST P-256 pentru certificatele emise începând cu 01.03.2027.

Perechea de chei se generează în dispozitivul criptografic al titularului, tokenul certificat Century Longmai mToken CryptoID (dispozitiv calificat de creare a semnăturilor și a sigiliilor; FIPS 140-3, nivelul de securitate 3, certificatul CMVP nr. 4845): fie de CERTDIGITAL, la emitere, fie de titular, prin aplicația CertDigital CSR. Cheia privată nu părăsește dispozitivul. CERTDIGITAL nu păstrează, nu arhivează și nu poate recupera cheile private ale titularilor.

2.3. Verificarea identității

Înainte de emiterea unui certificat calificat, CERTDIGITAL verifică identitatea titularului și, după caz, atributele persoanei juridice, prin una dintre următoarele metode:

a) **prin prezență fizică**, în fața unui operator de înregistrare CERTDIGITAL, cu actul de identitate, pașaportul sau permisul de ședere, în original (art. 24 alin. (1a) lit. (d) din Regulamentul eIDAS; art. 16 alin. (3) lit. a) din Legea nr. 214/2024);

b) **la distanță, prin soluția CERTDIGITAL KYC**: înregistrare video realizată de titular, cu verificarea automatizată a documentului de identitate și a persoanei, urmată de verificarea înregistrării de către un operator CERTDIGITAL în cel mult 24 de ore. Soluția este înscrisă de ADR în Lista terților de verificare a identității persoanei la distanță utilizând mijloace video. Compararea biometrică a imaginii faciale se face numai cu consimțământul explicit al titularului;

c) **pe baza unui certificat calificat CERTDIGITAL valabil**, emis după verificarea identității prin una dintre metodele de la lit. a) sau b), numai pentru reînnoire (art. 24 alin. (1a) lit. (b) din Regulamentul eIDAS).

Pentru cetățenii români, valabilitatea actului de identitate se verifică prin Platforma națională de interoperabilitate. Pentru certificatele de sigiliu și pentru titularii asociați unei persoane juridice se verifică și existența persoanei juridice și calitatea reprezentantului. Începând cu 19.08.2027, verificarea identității respectă și Regulamentul de punere în aplicare (UE) 2025/1566 (ETSI TS 119 461 V2.1.1).

2.4. Certificatele pentru chei gestionate în QSCD la distanță

Certificatele asociate cheilor generate și gestionate de CERTDIGITAL într-un dispozitiv calificat la distanță au identificatorii 1.3.6.1.4.1.47898.4.2.2.{1,4,6}.{1,2} în generația G4, respectiv 1.3.6.1.4.1.47898.5.2.2.{1,4,6}.{1,2} în generația G5, identificatorul 1.3.6.1.4.1.47898.11.1.1 (chei de lungă durată) sau 1.3.6.1.4.1.47898.11.1.2 (chei de unică folosință) și politica EUSPv2 (0.4.0.19431.1.1.4). Ele sunt supuse, în plus, Termenilor și condițiilor serviciului de gestionare la distanță a QSCD (TC-rQSCD) și Politicii și declarației de practici a serviciului (PDP-rQSCD).

Cheile de unică folosință se generează, se certifică, se utilizează și se șterg pe baza unei singure autorizări a titularului, într-o singură sesiune de semnare, iar cheia se șterge imediat după încheierea sesiunii. Certificatele lor sunt certificate calificate de scurtă durată (ETSI EN 319 411-1, clauza 3.1), valabile cel mult 60 de minute de la emitere, fără antedatare, și se emit după o nouă verificare a identității titularului. Ele sunt revocabile, în aceleași condiții ca celelalte certificate (secțiunea 2.6), iar starea lor este disponibilă prin OCSP și CRL și după expirare; ștergerea cheii nu revocă certificatul. Cheile de unică folosință și certificatele lor nu se reînnoiesc. Semnăturile create cu aceste certificate conțin o marcă temporală calificată aplicată în perioada de valabilitate a certificatului.

2.5. Certificatele de serviciu ale CERTDIGITAL

CERTDIGITAL QCA G5 emite, pentru serviciile de încredere ale CERTDIGITAL, certificate calificate pentru sigiliul electronic al căror titular este CENTRUL DE CALCUL S.A. Cheile acestor certificate sunt generate în ceremonie și păstrate în modulul criptografic al CERTDIGITAL. Fiecare certificat se folosește numai pentru serviciul indicat:

Certificatul	Utilizarea	Politicile
CERTDIGITAL TSA G5	semnarea mărcilor temporale calificate (extKeyUsage timeStamping)	QCP-l-qscd (0.4.0.194112.1.3) și 1.3.6.1.4.1.47898.5.2.2.1.2
CERTDIGITAL QPS SERVICE G5	păstrarea calificată a semnăturilor și a sigiliilor electronice calificate	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.10.1
CERTDIGITAL QESVAL SERVICE G5	validarea calificată a semnăturilor și a sigiliilor electronice calificate	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.9.1
CERTDIGITAL QEARCH SERVICE G5	arhivarea electronică calificată	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.12.1
CERTDIGITAL QLEDGERS SERVICE G5	registrele electronice calificate	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.13.1
CERTDIGITAL QERDS SERVICE G5	transmiterea electronică înregistrată calificată	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.14.1
CERTDIGITAL QREM SERVICE G5	poșta electronică înregistrată calificată (extKeyUsage emailProtection)	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.14.1
CERTDIGITAL QEAA SERVICE G5	atestarea electronică calificată a atributelor (cheie ECDSA P-256)	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 și 1.3.6.1.4.1.47898.15.1

Aceste certificate conțin declarațiile QcCompliance, QcSSCD, QcType eSeal și QcPDS, cu aceleași adrese ca certificatele titularilor, și sunt valabile 5 ani; certificatul CERTDIGITAL TSA G5 este valabil 3 ani, iar cheia lui se utilizează cel mult 2 ani. Certificatul CERTDIGITAL OCSP G5, valabil 3 ani, semnează numai răspunsurile OCSP; nu este certificat calificat și nu conține declarații QC. Certificatele de serviciu emise de CERTDIGITAL QUALIFIED CA G4 sunt descrise în IER-PKI; declarația lor QcPDS trimite la pagina depozitului.

2.6. Utilizarea, reînnoirea și revocarea

Certificatul calificat pentru semnătura electronică se folosește pentru crearea și validarea semnăturilor electronice calificate ale persoanei fizice titulare și pentru autentificarea acesteia; certificatul calificat pentru sigiliul electronic, pentru crearea și validarea sigiliilor electronice calificate ale persoanei juridice titulare și pentru autentificarea acesteia. Certificatele nu se utilizează:

– în afara scopurilor indicate în extensiile keyUsage și extKeyUsage și în politica de certificare;

– după expirare sau revocare;

– pentru emiterea de certificate sau de liste de revocare;

– în sisteme de control ale instalațiilor critice, în care o defecțiune poate provoca decese, vătămări sau daune grave asupra mediului;

– pentru activități ilegale.

Certificatul se consideră acceptat de titular la prima sa utilizare sau, în lipsa unei obiecții, la împlinirea a 7 zile calendaristice de la punerea sa la dispoziție. Reînnoirea se face numai cu generarea unei perechi noi de chei; reînnoirea la distanță, pe baza certificatului calificat CERTDIGITAL valabil, este permisă o singură dată consecutiv.

Revocarea se publică imediat prin serviciul OCSP și se include în următoarea CRL, emisă cel târziu în 24 de ore. Titularul este informat de îndată, cu indicarea motivelor. CERTDIGITAL nu oferă serviciul de suspendare a certificatelor: în situațiile în care legea prevede suspendarea (art. 17 alin. (1) din Legea nr. 214/2024), certificatul se revocă. Registrul public al certificatelor (https://ca.certdigital.ro/registry) indică, pentru fiecare certificat, starea și, după caz, data, ora și motivul revocării.

3. Limitele de încredere

Certificatele nu conțin limite de valoare a tranzacțiilor (nu conțin declarația QcLimitValue). Limitele de utilizare sunt cele de la secțiunea 2.6 și sunt indicate în certificat prin extensiile keyUsage și extKeyUsage, prin politica de certificare și prin perioada de valabilitate.

CERTDIGITAL păstrează certificatele emise, documentele și datele utilizate la verificarea identității (inclusiv înregistrările video realizate prin CERTDIGITAL KYC), cererile, înregistrările de revocare și jurnalele de evenimente relevante cel puțin 10 ani de la încetarea valabilității certificatului (art. 16 alin. (2) din Legea nr. 214/2024; art. 24 alin. (2) lit. (h) din Regulamentul eIDAS). În caz de încetare a activității, înregistrările sunt păstrate și puse la dispoziție conform Planului de încetare a serviciilor.

Serviciile de informare privind starea certificatelor (OCSP și CRL) sunt disponibile 24 de ore din 24, 7 zile din 7, cu o disponibilitate-țintă de 99,5% pe an. Informațiile privind starea certificatelor sunt gratuite și rămân disponibile și după expirarea certificatelor (art. 24 alin. (4) din Regulamentul eIDAS).

4. Obligațiile titularului și ale abonatului

Titularul și, după caz, abonatul au următoarele obligații:

– să furnizeze date exacte, complete și actuale și să comunice de îndată orice modificare a acestora;

– să ia cunoștință de termenii și condițiile (TC-CERT) înainte de încheierea contractului; abonatul care contractează certificate pentru angajații sau reprezentanții săi se asigură că aceștia iau cunoștință de ele;

– să păstreze dispozitivul criptografic și datele de activare (codurile PIN și PUK) sub controlul său exclusiv și să nu le divulge;

– atunci când își generează singur cheile, să folosească numai dispozitivele criptografice și aplicația CertDigital CSR indicate de CERTDIGITAL;

– să verifice datele din certificat la primire și să semnaleze imediat orice neconcordanță;

– să utilizeze certificatul numai în scopurile permise (secțiunea 2.6) și numai în perioada de valabilitate;

– să solicite revocarea certificatului în cel mult 24 de ore de la pierderea sau compromiterea dispozitivului ori a datelor de activare, sau de la constatarea că datele din certificat nu mai corespund realității (art. 26 din Legea nr. 214/2024);

– să înceteze imediat și definitiv utilizarea cheii private în cazul compromiterii acesteia, precum și după expirarea sau revocarea certificatului ori după ce a fost informat despre compromiterea autorității de certificare;

– pentru certificatele de sigiliu: persoana juridică titulară stabilește persoanele care utilizează sigiliul, notifică încetarea calității acestora și răspunde de utilizarea sigiliului.

5. Obligațiile părților care se bazează

Înainte de a se baza pe un certificat sau pe o semnătură ori un sigiliu creat cu acesta, partea care se bazează:

– verifică starea certificatului la momentul semnării, prin OCSP sau prin cea mai recentă CRL (secțiunea 1.2);

– verifică lanțul de certificare până la autoritatea rădăcină (CERTDIGITAL ROOT CA G4 sau CERTDIGITAL ROOT CA G5, după autoritatea emitentă), folosind certificatele autorităților publicate de CERTDIGITAL (secțiunea 1.2);

– verifică statutul calificat al serviciului în Lista de încredere a României (https://trustedlist.adr.gov.ro/);

– respectă limitările de utilizare indicate în certificat (keyUsage, extKeyUsage, politica de certificare) și în prezentul document;

– validează semnătura sau sigiliul conform ETSI EN 319 102-1 (de exemplu, prin intermediul unui serviciu de validare) și ține seama de marca temporală, acolo unde există, pentru stabilirea momentului semnării.

La cererea scrisă a oricărei persoane, însoțită de documentul semnat, CERTDIGITAL verifică gratuit dacă semnătura sau sigiliul a fost creat cu un certificat emis de CERTDIGITAL, starea certificatului la momentul semnării și integritatea semnăturii, și comunică rezultatul în cel mult 30 de zile (art. 11 alin. (2) din Legea nr. 214/2024). Această verificare nu constituie un serviciu calificat de validare.

6. Garanția limitată și limitarea răspunderii

CERTDIGITAL răspunde, conform art. 13 din Regulamentul eIDAS și art. 30 din Legea nr. 214/2024, pentru prejudiciile cauzate cu intenție sau din neglijență oricărei persoane fizice sau juridice, inclusiv titularilor și părților care se bazează, prin nerespectarea obligațiilor care îi revin. Intenția sau neglijența CERTDIGITAL se prezumă, cu excepția cazului în care CERTDIGITAL dovedește că prejudiciul s-a produs fără intenția sau neglijența sa.

CERTDIGITAL nu răspunde pentru prejudiciile rezultate din:

– utilizarea certificatului peste limitările notificate în prealabil și recognoscibile de terți (art. 13 alin. (2) din Regulamentul eIDAS; art. 15 alin. (5) din Legea nr. 214/2024);

– nerespectarea de către titular a obligațiilor sale (capitolul 4);

– neverificarea de către partea care se bazează a stării certificatului și a statutului din Lista de încredere;

– forța majoră.

Răspunderea pentru prejudiciile cauzate cu intenție sau din culpă gravă nu este exclusă și nu este limitată (art. 1355 din Codul civil); în raporturile cu consumatorii se aplică Legea nr. 193/2000.

CENTRUL DE CALCUL S.A. deține, pentru fiecare dintre cele două servicii de certificare calificată (certificate calificate pentru semnătura electronică și certificate calificate pentru sigiliul electronic), câte o poliță distinctă de asigurare de răspundere civilă profesională, cu limita răspunderii de 500.000 EUR pe perioada asigurată (art. 12 alin. (6) din Legea nr. 214/2024); în fiecare poliță, ADR are calitatea de asigurat adițional.

7. Documentele aplicabile

Următoarele documente se aplică împreună cu prezentul document, în versiunea în vigoare:

– Politica serviciilor de certificare CertDigital;

– Declarația practicilor de certificare a CERTDIGITAL ROOT CA G4 și CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4);

– Declarația practicilor de certificare a CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5 (DPC CERTDIGITAL G5);

– Termenii și condițiile pentru certificatele calificate (TC-CERT);

– Contractul de furnizare a serviciilor de certificare calificată (CTR-CERT);

– Politicile generale ale prestatorului de servicii de încredere;

– Ierarhia PKI CertDigital și politicile sprijinite (IER-PKI);

– Politica și declarația de practici a serviciului de gestionare la distanță a QSCD (PDP-rQSCD) și termenii și condițiile serviciului (TC-rQSCD);

– Politicile și declarațiile de practici ale serviciilor care folosesc certificatele de serviciu G5: PDP-QTST, PSPPS (QPS), PDP-QESVal, PDP-QEArch, PDP-Ledgers, PDP-QERDS (QeRDS și QREM), PDP-QEAA;

– Politica de protecție a datelor cu caracter personal;

– Planul de încetare a serviciilor.

Documentele publice sunt în depozitul https://www.certdigital.ro/repository/, iar versiunile lor anterioare, în arhiva depozitului. Contractul se pune la dispoziția beneficiarului înainte de semnare.

8. Protecția datelor cu caracter personal

Operatorul datelor este CENTRUL DE CALCUL S.A. (CertDigital). Datele de identificare și de contact ale titularului și ale reprezentanților, copia actului de identitate și, la identificarea la distanță, înregistrarea video se prelucrează pentru verificarea identității, emiterea și gestionarea certificatului, în temeiul contractului și al obligațiilor legale (art. 6 alin. (1) lit. b) și c) din Regulamentul (UE) 2016/679; Regulamentul eIDAS; Legea nr. 214/2024). Compararea biometrică din CERTDIGITAL KYC se face numai cu consimțământul explicit al titularului. Datele se păstrează cel puțin 10 ani de la încetarea valabilității certificatului.

Certificatul conține datele de identificare ale titularului, publicate în registrul certificatelor; registrul nu afișează codul numeric personal, iar certificatul complet poate fi descărcat din registru numai cu acordul titularului. Certificatele de semnătură conțin și extensia 1.3.6.1.4.1.47898.30.1, care leagă certificatul de documentul de identitate verificat printr-o amprentă a datelor acestuia, fără datele în clar.

Persoanele vizate au dreptul de acces, rectificare, ștergere (în limitele legii), restricționare, portabilitate și opoziție, precum și dreptul de a depune plângere la ANSPDCP. Responsabilul cu protecția datelor: dpo@centruldecalcul.ro. Detalii: Politica de protecție a datelor cu caracter personal, publicată la https://www.certdigital.ro/protectia-datelor/.

9. Tarifele și rambursarea

Tarifele serviciilor sunt cele din lista de tarife publicată pe site-ul https://www.certdigital.ro/ sau din oferta transmisă la cerere (art. 11 alin. (3) lit. b) din Legea nr. 214/2024). Informațiile privind starea certificatelor (OCSP, CRL), consultarea registrului certificatelor, revocarea și verificarea unei semnături la cererea unui terț sunt gratuite. Rambursările se fac conform contractului și, pentru consumatori, conform Ordonanței de urgență a Guvernului nr. 34/2014.

10. Legea aplicabilă, reclamațiile și soluționarea litigiilor

Serviciile sunt furnizate în conformitate cu Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183, cu actele de punere în aplicare aplicabile (între care Regulamentul de punere în aplicare (UE) 2025/1943), cu Legea nr. 214/2024, cu Ordinul MEDAT nr. 102/2026 și cu Regulamentul (UE) 2016/679. Lista completă a actelor normative și a standardelor aplicate se află în DPC CERTDIGITAL G4 și în DPC CERTDIGITAL G5, secțiunea 9.15. Contractul este guvernat de dreptul român.

Reclamațiile se transmit la office@certdigital.ro, iar CERTDIGITAL răspunde în cel mult 30 de zile. În lipsa unei soluții amiabile, litigiile cu profesioniștii sunt de competența instanțelor de la sediul CENTRUL DE CALCUL S.A. (Târgu Jiu). Consumatorii se pot adresa instanțelor competente potrivit legii, inclusiv celor de la domiciliul lor, și pot apela la procedurile de soluționare alternativă a litigiilor (SAL) prevăzute de Ordonanța Guvernului nr. 38/2015 (ANPC – https://anpc.ro/sal). Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

11. Statutul calificat, evaluarea conformității și auditul

CENTRUL DE CALCUL S.A. este prestator de servicii de încredere calificat, înscris în Lista de încredere a României (https://trustedlist.adr.gov.ro/), pentru serviciile de emitere a certificatelor calificate pentru semnătura electronică și pentru sigiliul electronic. Statutul calificat se verifică în Lista de încredere și în EU Trust Services Dashboard (https://eidas.ec.europa.eu/efda/).

Serviciile sunt evaluate cel puțin o dată la 24 de luni de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162 (EN ISO/IEC 17065 completat de ETSI EN 319 403-1) (art. 20 din Regulamentul eIDAS); atestarea de conformitate se publică la https://www.certdigital.ro/repository/conformitate/ după emitere, alături de deciziile ADR privind statutul calificat. CERTDIGITAL efectuează anual un audit intern.