

Declarația practicilor de certificare a CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5

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	Ofițer de Securitate IT	Prima versiune: declarația practicilor de certificare a generației G5 (CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5), după modelul DPC CERTDIGITAL G4 v2.0: modulele Thales Luna PCIe HSM 7 A790 (partițiile ROOTG5, CAG5 și SVG5), ceremonia unică de generare a cheilor, profilurile G5 (politicile din arcul 1.3.6.1.4.1.47898.5), CRL-urile și serviciul OCSP G5	26/10/2026
1.1	Ofițer de Securitate IT	Serviciul de gestionare la distanță a QSCD e descris ca serviciu pentru care se solicită statutul calificat (art. 21 alin. (3) din Regulamentul eIDAS); legătura ANPC pentru SAL devine https://anpc.ro/sal; trimiterile la documentele asociate, la versiunile în vigoare (PC v2.1, DPC CERTDIGITAL G4 v2.1, PDS v2.1, PDP-rQSCD v2.2); tabelul de identificare arată versiunea în vigoare	27/10/2026
1.2	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	27/10/2026
1.3	Ofițer de Securitate IT	Secțiunea 6.1.1 descrie ceremonia cheilor G5 ca încheiată (23.10.2026, procesele-verbale nr. 68658–68661), în acord cu secțiunea 7.1.11; pagina de emitere și antetul, cu diacritice	28/10/2026
1.4	Ofițer de Securitate IT	Centrele de date: în clădiri separate din același municipiu (5.1.1); procedura de generare a cheilor numită exact (5.2.2, 6.1.1); abaterile ceremoniei din 23.10.2026 și ceremonia de remediere (relocarea cheilor, cheia QEAA generată din nou în SVG5) (6.1.1)	02/11/2026
1.5	Ofițer de Securitate IT	Cheile de semnare de unică folosință din serviciul rQSCD: certificatele calificate de scurtă	02/11/2026

		durată, valabile cel mult 60 de minute de la emitere, fără antedatare, cu identificatorul 1.3.6.1.4.1.47898.11.1.2 și codurile de identificare 1 sau 4, revocabile, cu starea în CRL și OCSP și după expirare, fără extensia validity-assured (1.2, 1.6.1, 4.9.3, 4.10.1, 6.3.2, 7.1.2); verificarea identității pentru fiecare certificat, emiterea și acceptarea în sesiune, fără reînnoire (3.2.1, 3.2.3, 3.3.1, 4.2.3, 4.3.1, 4.4.1, 4.7.1); generarea și activarea într-o singură sesiune, ștergerea cheii imediat după aceasta și marca temporală calificată a semnăturilor (4.5.2, 4.12.1, 5.4.1, 6.1.1, 6.2.4, 6.2.8–6.2.10, 6.3.2)	

Cuprins

1. Introducere 14
1.1. Prezentare generală 14
1.2. Denumirea și identificarea documentului 15
1.3. Participanții la infrastructura de chei publice 16
1.3.1. Autoritățile de certificare 16
1.3.2. Autoritatea de înregistrare 17
1.3.3. Titularii 17
1.3.4. Părțile care se bazează 17
1.3.5. Alți participanți 18
1.4. Utilizarea certificatelor 18
1.4.1. Utilizările permise 18
1.4.2. Utilizările interzise 18
1.4.3. Certificatele de test 19
1.5. Administrarea politicii 19
1.5.1. Organizația care administrează documentul 19
1.5.2. Persoana de contact 19
1.5.3. Persoana care stabilește conformitatea DPC cu politica 19
1.5.4. Procedura de aprobare a DPC 19
1.6. Definiții și acronime 20
1.6.1. Definiții 20
1.6.2. Acronime 20
2. Responsabilitățile privind publicarea și depozitul 21
2.1. Depozitele 21
2.2. Publicarea informațiilor 21
2.3. Momentul sau frecvența publicării 21
2.4. Controlul accesului la depozite 22
3. Identificarea și autentificarea 23
3.1. Denumirea 23

3.1.1. Tipuri de nume 23
3.1.2. Necesitatea ca numele să fie semnificative 23
3.1.3. Anonimatul sau pseudonimul titularilor 24
3.1.4. Reguli de interpretare a diferitelor forme de nume 24
3.1.5. Unicitatea numelor 24
3.1.6. Recunoașterea, autentificarea și rolul mărcilor înregistrate 24
3.2. Validarea inițială a identității 24
3.2.1. Metoda de dovedire a deținerii cheii private 24
3.2.2. Autentificarea identității organizației 24
3.2.3. Autentificarea identității persoanelor fizice 25
3.2.4. Informațiile neverificate ale titularului 26
3.2.5. Validarea autorității 26
3.2.6. Criterii de interoperabilitate 26
3.3. Identificarea și autentificarea pentru reînnoirea cheii 26
3.3.1. Reînnoirea de rutină a cheii 26
3.3.2. Reînnoirea cheii după revocare 27
3.4. Identificarea și autentificarea pentru cererea de revocare 27
4. Cerințe operaționale privind ciclul de viață al certificatelor 28
4.1. Cererea de certificat 28
4.1.1. Cine poate depune o cerere 28
4.1.2. Procesul de înregistrare și responsabilitățile 28
4.2. Prelucrarea cererii 28
4.2.1. Efectuarea identificării și autentificării 28
4.2.2. Aprobarea sau respingerea cererii 28
4.2.3. Durata de prelucrare a cererii 28
4.3. Emiterea certificatului 29
4.3.1. Acțiunile CA în timpul emiterii 29
4.3.2. Notificarea titularului 29
4.4. Acceptarea certificatului 29
4.4.1. Modul de acceptare 29
4.4.2. Publicarea certificatului de către CA 29
4.4.3. Notificarea altor entități 30

4.5. Utilizarea perechii de chei și a certificatului 30
4.5.1. Utilizarea cheii private și a certificatului de către titular 30
4.5.2. Utilizarea cheii publice și a certificatului de către partea care se bazează 30
4.6. Reînnoirea certificatului (fără schimbarea cheii) 31
4.6.1. Circumstanțele reînnoirii 31
4.6.2. Cine poate solicita reînnoirea 31
4.6.3. Prelucrarea cererii de reînnoire 31
4.6.4. Notificarea titularului 31
4.6.5. Modul de acceptare 31
4.6.6. Publicarea certificatului reînnoit 31
4.6.7. Notificarea altor entități 31
4.7. Reînnoirea cu schimbarea cheii 31
4.7.1. Circumstanțele 31
4.7.2. Cine poate solicita 31
4.7.3. Prelucrarea cererii 31
4.7.4. Notificarea titularului 32
4.7.5. Modul de acceptare 32
4.7.6. Publicarea certificatului 32
4.7.7. Notificarea altor entități 32
4.8. Modificarea certificatului 32
4.8.1. Circumstanțele 32
4.8.2. Cine poate solicita modificarea 32
4.8.3. Prelucrarea cererii 32
4.8.4. Notificarea titularului 32
4.8.5. Modul de acceptare 32
4.8.6. Publicarea certificatului modificat 32
4.8.7. Notificarea altor entități 32
4.9. Revocarea și suspendarea certificatului 32
4.9.1. Circumstanțele revocării 32
4.9.2. Cine poate solicita revocarea 33
4.9.3. Procedura de revocare 33
4.9.4. Perioada de grație pentru cererea de revocare 34

4.9.5. Termenul în care CA trebuie să prelucreze cererea 34
4.9.6. Cerințe de verificare a revocării pentru părțile care se bazează 34
4.9.7. Frecvența emiterii CRL 35
4.9.8. Latența maximă a CRL 35
4.9.9. Disponibilitatea verificării online a stării 35
4.9.10. Cerințe pentru verificarea online 35
4.9.11. Alte forme de anunțare a revocării 35
4.9.12. Cerințe speciale privind compromiterea cheii 36
4.9.13. Circumstanțele suspendării 36
4.9.14. Cine poate solicita suspendarea 36
4.9.15. Procedura de suspendare 36
4.9.16. Limitele perioadei de suspendare 36
4.10. Serviciile privind starea certificatelor 36
4.10.1. Caracteristici operaționale 36
4.10.2. Disponibilitatea serviciului 37
4.10.3. Caracteristici opționale 37
4.11. Încetarea contractului 37
4.12. Păstrarea în custodie și recuperarea cheilor 37
4.12.1. Politica și practicile de custodie și recuperare a cheilor 37
4.12.2. Politica și practicile de încapsulare și recuperare a cheilor de sesiune 37
5. Controale privind facilitățile, managementul și operarea 38
5.1. Controale fizice 38
5.1.1. Amplasarea și construcția 38
5.1.2. Accesul fizic 38
5.1.3. Alimentarea cu energie și climatizarea 38
5.1.4. Expunerea la apă 38
5.1.5. Prevenirea și protecția împotriva incendiilor 38
5.1.6. Păstrarea suporturilor de stocare 38
5.1.7. Eliminarea deșeurilor 39
5.1.8. Copiile de rezervă în afara locației 39
5.2. Controale procedurale 39
5.2.1. Rolurile de încredere 39

5.2.2. Numărul de persoane necesare pentru fiecare activitate 39
5.2.3. Identificarea și autentificarea pentru fiecare rol 40
5.2.4. Rolurile care necesită separarea sarcinilor 40
5.3. Controale privind personalul 40
5.3.1. Calificări, experiență și autorizări 40
5.3.2. Verificarea antecedentelor 40
5.3.3. Instruirea 40
5.3.4. Frecvența reinstruirii 40
5.3.5. Rotația posturilor 40
5.3.6. Sancțiuni pentru acțiuni neautorizate 40
5.3.7. Cerințe pentru personalul extern 41
5.3.8. Documentația pusă la dispoziția personalului 41
5.4. Procedurile de jurnalizare pentru audit 41
5.4.1. Tipurile de evenimente înregistrate 41
5.4.2. Frecvența prelucrării jurnalelor 41
5.4.3. Perioada de păstrare a jurnalelor 41
5.4.4. Protecția jurnalelor 41
5.4.5. Copiile de rezervă ale jurnalelor 41
5.4.6. Sistemul de colectare 42
5.4.7. Notificarea persoanei care a generat evenimentul 42
5.4.8. Evaluarea vulnerabilităților 42
5.5. Arhivarea înregistrărilor 42
5.5.1. Tipurile de înregistrări arhivate 42
5.5.2. Perioada de păstrare 42
5.5.3. Protecția arhivei 42
5.5.4. Copiile de rezervă ale arhivei 42
5.5.5. Marcarea temporală a înregistrărilor 42
5.5.6. Sistemul de colectare a arhivei 43
5.5.7. Proceduri de obținere și verificare a informațiilor din arhivă 43
5.6. Schimbarea cheii autorității 43
5.7. Compromiterea și recuperarea în caz de dezastru 43
5.7.1. Gestionarea incidentelor și a compromiterii 43

5.7.2. Coruperea resurselor, a programelor sau a datelor 44
5.7.3. Compromiterea cheii private a autorității 44
5.7.4. Continuitatea activității după un dezastru 44
5.8. Încetarea activității CA sau RA 44
6. Controale tehnice de securitate 46
6.1. Generarea și instalarea perechii de chei 46
6.1.1. Generarea perechii de chei 46
6.1.2. Livrarea cheii private către titular 47
6.1.3. Livrarea cheii publice către emitentul certificatului 47
6.1.4. Livrarea cheii publice a CA către părțile care se bazează 47
6.1.5. Dimensiunea cheilor 47
6.1.6. Generarea parametrilor cheii publice și verificarea calității 48
6.1.7. Scopurile utilizării cheii (keyUsage X.509 v3) 48
6.2. Protecția cheii private și controalele modulului criptografic 49
6.2.1. Standardele și controalele modulului criptografic 49
6.2.2. Controlul multipersoană (M din N) al cheii private 49
6.2.3. Păstrarea în custodie a cheii private 49
6.2.4. Copia de rezervă a cheii private 49
6.2.5. Arhivarea cheii private 50
6.2.6. Transferul cheii private în sau din modulul criptografic 50
6.2.7. Stocarea cheii private în modulul criptografic 50
6.2.8. Metoda de activare a cheii private 50
6.2.9. Metoda de dezactivare a cheii private 50
6.2.10. Metoda de distrugere a cheii private 51
6.2.11. Evaluarea modulului criptografic 51
6.3. Alte aspecte ale gestionării perechii de chei 52
6.3.1. Arhivarea cheii publice 52
6.3.2. Perioadele de valabilitate ale certificatelor și de utilizare a cheilor 52
6.4. Datele de activare 52
6.4.1. Generarea și instalarea datelor de activare 52
6.4.2. Protecția datelor de activare 52
6.4.3. Alte aspecte ale datelor de activare 53

6.5. Controale de securitate a sistemelor informatice 53
6.5.1. Cerințe tehnice specifice 53
6.5.2. Evaluarea securității sistemelor 53
6.6. Controale tehnice privind ciclul de viață 53
6.6.1. Controlul dezvoltării sistemelor 53
6.6.2. Controlul gestionării securității 53
6.6.3. Controalele de securitate ale ciclului de viață 53
6.7. Controale de securitate a rețelei 53
6.8. Marcarea temporală 54
7. Profilurile certificatelor, CRL și OCSP 55
7.1. Profilul certificatelor 55
7.1.1. Numărul versiunii 55
7.1.2. Extensiile certificatelor 55
7.1.3. Identificatorii algoritmilor 58
7.1.4. Formele de nume 59
7.1.5. Constrângerile de nume 59
7.1.6. Identificatorul politicii de certificare 59
7.1.7. Utilizarea extensiei policyConstraints 59
7.1.8. Sintaxa și semantica calificativelor de politică 59
7.1.9. Prelucrarea extensiei certificatePolicies critice 59
7.1.10. Diferențele față de profilurile generației G4 59
7.1.11. Certificatele emise la ceremonia din 23.10.2026 60
7.2. Profilul CRL 60
7.2.1. Numărul versiunii 60
7.2.2. Extensiile CRL și ale intrărilor 61
7.3. Profilul OCSP 61
7.3.1. Numărul versiunii 61
7.3.2. Extensiile OCSP 61
8. Evaluarea conformității și alte evaluări 62
8.1. Frecvența sau circumstanțele evaluării 62
8.2. Identitatea și calificarea evaluatorului 62
8.3. Relația evaluatorului cu entitatea evaluată 62

8.4. Subiectele acoperite de evaluare 62
8.5. Acțiunile întreprinse ca urmare a neconformităților 62
8.6. Comunicarea rezultatelor 62
9. Alte aspecte comerciale și juridice 63
9.1. Tarife 63
9.1.1. Tarifele pentru emiterea sau reînnoirea certificatelor 63
9.1.2. Tarifele pentru accesul la certificate 63
9.1.3. Tarifele pentru accesul la informațiile de revocare sau de stare 63
9.1.4. Tarifele pentru alte servicii 63
9.1.5. Politica de rambursare 63
9.2. Responsabilitatea financiară 63
9.2.1. Acoperirea prin asigurare 63
9.2.2. Alte active 63
9.2.3. Asigurarea sau garanția pentru entitățile finale 63
9.3. Confidențialitatea informațiilor comerciale 64
9.3.1. Domeniul informațiilor confidențiale 64
9.3.2. Informațiile care nu sunt confidențiale 64
9.3.3. Responsabilitatea pentru protejarea informațiilor confidențiale 64
9.4. Protecția datelor cu caracter personal 64
9.4.1. Politica de confidențialitate 64
9.4.2. Informațiile tratate ca private 64
9.4.3. Informațiile care nu sunt considerate private 64
9.4.4. Responsabilitatea pentru protejarea datelor 64
9.4.5. Notificarea și consimțământul pentru utilizarea datelor 65
9.4.6. Dezvăluirea în cadrul procedurilor judiciare sau administrative 65
9.4.7. Alte situații de dezvăluire 65
9.5. Drepturile de proprietate intelectuală 65
9.6. Declarații și garanții 65
9.6.1. Declarațiile și garanțiile CA 65
9.6.2. Declarațiile și garanțiile RA 65
9.6.3. Declarațiile și garanțiile titularilor 65
9.6.4. Declarațiile și garanțiile părților care se bazează 66

9.6.5. Declarațiile și garanțiile altor participanți 66
9.7. Exonerarea de garanții 66
9.8. Limitarea răspunderii 66
9.9. Despăgubiri 66
9.10. Durata și încetarea 66
9.10.1. Durata 66
9.10.2. Încetarea 66
9.10.3. Efectul încetării și dispozițiile care rămân aplicabile 67
9.11. Notificările individuale și comunicarea cu participanții 67
9.12. Modificări 67
9.12.1. Procedura de modificare 67
9.12.2. Mecanismul și termenul de notificare 67
9.12.3. Circumstanțele în care trebuie schimbat identificatorul de politică 67
9.13. Soluționarea litigiilor 67
9.14. Legea aplicabilă 68
9.15. Conformitatea cu legislația aplicabilă 68
9.16. Dispoziții diverse 69
9.16.1. Întregul acord 69
9.16.2. Cesiunea 69
9.16.3. Separabilitatea 69
9.16.4. Executarea 69
9.16.5. Forța majoră 69
9.17. Alte prevederi 69

1. Introducere

1.1. Prezentare generală

Prezentul document este Declarația practicilor de certificare (DPC) a autorităților de certificare din generația G5 a infrastructurii de chei publice CERTDIGITAL: autoritatea rădăcină **CERTDIGITAL ROOT CA G5** și autoritatea subordonată **CERTDIGITAL QCA G5**, operate de CENTRUL DE CALCUL S.A. (denumită în continuare „CERTDIGITAL"), prestator de servicii de încredere calificat. Documentul descrie practicile aplicate pentru generarea și protecția cheilor celor două autorități, pentru emiterea certificatului CERTDIGITAL QCA G5 de către autoritatea rădăcină și pentru emiterea și gestionarea, de către CERTDIGITAL QCA G5:

– certificatelor calificate pentru semnătura electronică, emise persoanelor fizice;

– certificatelor calificate pentru sigiliul electronic, emise persoanelor juridice;

– certificatelor calificate pentru semnătura și sigiliul electronic ale căror chei sunt generate și gestionate de CERTDIGITAL, în numele titularului, într-un dispozitiv calificat la distanță (serviciul de gestionare la distanță a QSCD, pentru care se solicită statutul calificat, descris în Politica și declarația de practici a serviciului rQSCD (PDP-rQSCD), OID 1.3.6.1.4.1.47898.11.1);

– certificatelor de serviciu ale prestatorului (OCSP, marcare temporală, validare, păstrare, arhivare, registre electronice, transmitere electronică înregistrată, atestare electronică a atributelor), emise, cu excepția certificatului OCSP, ca certificate calificate pentru sigiliul electronic al CENTRUL DE CALCUL S.A.

Documentul este structurat conform IETF RFC 3647 și respectă cerințele ETSI EN 319 411-1 V1.5.1 și ETSI EN 319 411-2 V2.6.1, astfel cum sunt referite în Regulamentul de punere în aplicare (UE) 2025/1943, precum și cerințele Regulamentului de punere în aplicare (UE) 2025/2530. Lista completă a standardelor aplicate se află în documentul „Lista standardelor aplicabile" (00n, versiunea în vigoare). Cerințele pe care le îndeplinesc certificatele sunt stabilite în Politica serviciilor de certificare CertDigital.

Generația G4 (CERTDIGITAL ROOT CA G4 și CERTDIGITAL QUALIFIED CA G4) funcționează în paralel și este descrisă în DPC CERTDIGITAL G4. Practicile comune celor două generații (identificarea și înregistrarea, revocarea, controalele fizice, procedurale și privind personalul, aspectele comerciale și juridice) sunt aceleași. Elementele proprii generației G5 sunt modulele criptografice și cheile autorităților (capitolul 6), profilurile certificatelor, ale listelor de revocare și ale serviciului OCSP (capitolul 7) și identificatorii politicilor (secțiunea 1.2).

Certificatele titularilor și certificatele de serviciu emise de CERTDIGITAL QCA G5 conform prezentei DPC, cu excepția certificatului CERTDIGITAL OCSP G5 (secțiunea 1.2), sunt

certificate calificate în sensul art. 3 pct. 15 și pct. 30 din Regulamentul (UE) nr. 910/2014 și îndeplinesc cerințele din anexele I și III la acesta. O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe (art. 25 alin. (2)); un sigiliu electronic calificat beneficiază de prezumția de integritate a datelor și de corectitudine a originii acestora (art. 35 alin. (2)).

1.2. Denumirea și identificarea documentului

Element	Valoare
Titlu	Declarația practicilor de certificare a CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5 (DPC CERTDIGITAL G5)
Referință internă	DPC-G5
Versiune	1.5
Data intrării în vigoare	data publicării în depozit, după aprobare
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_dpc-g5_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Politicile de certificare aplicate, identificate în certificate prin extensia certificatePolicies, sunt:

Tip de certificat	Politica ETSI (EN 319 411-2)	Politica CERTDIGITAL
Certificat calificat pentru semnătură electronică, persoană fizică	QCP-n-qscd (0.4.0.194112.1.2)	1.3.6.1.4.1.47898.5.1.{1,2}.{1,4,6}.1
Certificat calificat pentru sigiliu electronic, persoană juridică	QCP-l-qscd (0.4.0.194112.1.3)	1.3.6.1.4.1.47898.5.1.{1,2}.{1,4,6}.2
Certificat calificat pentru semnătură sau sigiliu, cu cheia gestionată de CERTDIGITAL în QSCD la distanță (serviciul rQSCD)	QCP-n-qscd (0.4.0.194112.1.2) / QCP-l-qscd (0.4.0.194112.1.3) și EUSPv2 (0.4.0.19431.1.1.4)	1.3.6.1.4.1.47898.5.2.2.{1,4,6}.{1,2} și 1.3.6.1.4.1.47898.11.1.1 (PDP-rQSCD, chei de lungă durată) sau 1.3.6.1.4.1.47898.11.1.2 (PDP-rQSCD, chei de unică folosință, certificate de scurtă durată)
Certificat de serviciu al prestatorului (sigiliu, cheie în HSM)	QCP-l-qscd (0.4.0.194112.1.3)	1.3.6.1.4.1.47898.5.2.2.1.2

Identificatorii CERTDIGITAL au structura `1.3.6.1.4.1.47898.5.{dispozitiv}.{generarea cheii}.{identificare}.{tip subiect}`:

– **dispozitiv:** 1 = dispozitivul criptografic al titularului (token USB); 2 = modul criptografic gestionat de CERTDIGITAL (HSM-ul certificatelor de serviciu sau dispozitivul calificat la distanță al serviciului rQSCD);

– **generarea cheii:** 1 = de titular, prin aplicația CertDigital CSR; 2 = de CERTDIGITAL;

– **identificare:** 1 = prezență fizică; 4 = la distanță, prin CERTDIGITAL KYC; 6 = pe baza unui certificat calificat CERTDIGITAL valabil (reînnoire);

– **tip subiect:** 1 = persoană fizică; 2 = persoană juridică.

Identificatorii generației G5 (arcul 1.3.6.1.4.1.47898.5) au aceeași structură ca identificatorii generației G4 (arcul 1.3.6.1.4.1.47898.4), descriși în DPC CERTDIGITAL G4. Lista completă a identificatorilor este ținută de CERTDIGITAL în CERTDIGITAL_OID_MAP. Un identificator nu se reutilizează cu alt sens; singura excepție este renumerotarea arcurilor serviciilor din 20–22.10.2026 (CERTDIGITAL_OID_MAP, secțiunea 18): identificatorul 1.3.6.1.4.1.47898.11.1, folosit cu sensul anterior în certificatul de serviciu QEArch G4, care se revocă (DPC CERTDIGITAL G4, secțiunea 7.1.2), identifică acum PDP-rQSCD.

Certificatele de serviciu G5, cu excepția certificatelor CERTDIGITAL TSA G5 și CERTDIGITAL OCSP G5, conțin, pe lângă politicile de mai sus, identificatorul politicii serviciului pentru care se folosesc (secțiunea 7.1.6). Certificatul CERTDIGITAL OCSP G5 nu este certificat calificat și conține numai identificatorul 1.3.6.1.4.1.47898.5.2.2.1.2.

Politicile „-qscd” și declarația QcSSCD se folosesc pentru certificatele ale căror chei se află pe tokenul certificat livrat de CERTDIGITAL, pentru emiterea în cloud, în HSM-ul cu modulul SAM atașat al serviciului rQSCD (secțiunea 6.2.11), și pentru certificatele de serviciu G5, cu excepția certificatului CERTDIGITAL OCSP G5, ale căror chei se află în modulele Thales Luna PCIe HSM 7 A790, certificate ca dispozitive calificate (secțiunea 6.2.1).

Pentru certificatele din serviciul rQSCD, cheia se află într-un dispozitiv calificat la distanță certificat și înscris pe lista Comisiei Europene (secțiunea 6.2.11), astfel că politicile „-qscd” și declarația QcSSCD sunt susținute. Aceste certificate se emit de la începerea serviciului rQSCD. Serviciul oferă chei de lungă durată, ale căror certificate sunt valabile cel mult 3 ani, și chei de unică folosință, generate pentru o singură sesiune de semnare și șterse imediat după încheierea ei. Certificatele cheilor de unică folosință sunt certificate calificate de scurtă durată, valabile cel mult 60 de minute (secțiunea 6.3.2), cu aceleași politici ca certificatele cheilor de lungă durată, dar cu identificatorul 1.3.6.1.4.1.47898.11.1.2 în locul identificatorului 1.3.6.1.4.1.47898.11.1.1 și numai cu codurile de identificare 1 sau 4, deoarece identitatea titularului se verifică din nou pentru fiecare certificat (secțiunea 3.2.3). Ele sunt revocabile (secțiunea 4.9.3).

1.3. Participanții la infrastructura de chei publice

1.3.1. Autoritățile de certificare

Ierarhia G5 a CERTDIGITAL are două niveluri:

Autoritate	Rol	Valabilitatea certificatului	Emitent
CERTDIGITAL ROOT CA G5	autoritate rădăcină, offline: partiția ei din modulul criptografic se activează numai în ceremonii; emite numai certificatul CERTDIGITAL QCA G5 și propria listă de revocare	25 de ani de la data ceremoniei de generare a cheii	autosemnat

Autoritate	Rol	Valabilitatea certificatului	Emitent
CERTDIGITAL QCA G5	autoritate subordonată care emite certificatele calificate și certificatele de serviciu descrise în prezenta DPC	15 ani de la data ceremoniei de generare a cheii	CERTDIGITAL ROOT CA G5

Data de început a valabilității fiecărui certificat este data ceremoniei în care se emite, fără antedatare. Numerele de serie, amprentele SHA-256 și datele exacte de valabilitate ale certificatelor se publică după ceremonie, în depozit și în documentul „Ierarhia PKI CertDigital" (IER-PKI, anexa B).

Certificatul CERTDIGITAL QCA G5 are constrângerea de lungime a căii 0 (nu poate emite alte autorități) și conține politica anyPolicy. Nu există certificare încrucișată cu alte autorități și nici între generațiile G4 și G5.

1.3.2. Autoritatea de înregistrare

Funcția de autoritate de înregistrare (RA) este îndeplinită exclusiv de operatori de înregistrare angajați ai CENTRUL DE CALCUL S.A., desemnați și instruiți, la sediul și la punctele de lucru ale CERTDIGITAL, precum și prin soluția proprie de identificare la distanță CERTDIGITAL KYC. CERTDIGITAL nu deleagă verificarea identității către terți. Autoritatea de înregistrare primește și verifică cererile de emitere, reînnoire și revocare, verifică identitatea solicitanților și aprobă sau respinge cererile.

1.3.3. Titularii

Titularul este persoana căreia i se emite certificatul și care deține cheia privată corespunzătoare:

– pentru certificatul de semnătură: persoana fizică identificată în certificat;

– pentru certificatul de sigiliu: persoana juridică identificată în certificat, reprezentată de reprezentantul său legal sau de o persoană împuternicită.

Solicitantul (abonatul) este persoana care încheie contractul cu CERTDIGITAL; el poate fi titularul însuși sau o persoană juridică ce solicită certificate pentru angajații ori reprezentanții săi, cu acordul acestora.

1.3.4. Părțile care se bazează

Partea care se bazează este orice persoană fizică sau juridică ce se bazează pe un certificat emis de CERTDIGITAL, de exemplu pentru verificarea unei semnături sau a unui sigiliu electronic. Partea care se bazează verifică starea certificatului (OCSP sau CRL), lanțul de certificare până la CERTDIGITAL ROOT CA G5, limitările de utilizare și statutul calificat al serviciului în Lista de încredere a României.

1.3.5. Alți participanți

– **furnizorii de dispozitive criptografice** (tokenuri USB), care livrează dispozitivele utilizate de titulari;

– **furnizorii de servicii de curierat**, care livrează titularilor, separat, dispozitivul și datele de activare;

– **organismul de evaluare a conformității** (CAB), care evaluează serviciul conform capitolului 8;

– **Autoritatea pentru Digitalizarea României (ADR)**, organism de supraveghere.

1.4. Utilizarea certificatelor

1.4.1. Utilizările permise

– certificatul calificat pentru semnătură electronică: crearea și validarea semnăturilor electronice calificate ale persoanei fizice titulare, precum și autentificarea titularului;

– certificatul calificat pentru sigiliu electronic: crearea și validarea sigiliilor electronice calificate ale persoanei juridice titulare, precum și autentificarea acesteia;

– certificatele de serviciu: semnarea răspunsurilor OCSP și a mărcilor temporale și sigilarea rapoartelor de validare, a dovezilor de păstrare, a pachetelor și rapoartelor de arhivare, a înregistrărilor din registrele electronice, a dovezilor de transmitere înregistrată și a atestatelor electronice ale atributelor emise de CERTDIGITAL, fiecare numai pentru serviciul indicat de politica serviciului din certificat (secțiunea 7.1.6) și, după caz, de extensia extKeyUsage; certificatele CERTDIGITAL OCSP G5 și CERTDIGITAL TSA G5 nu conțin o politică de serviciu, iar utilizarea lor rezultă numai din extKeyUsage (id-kp-OCSPSigning, respectiv id-kp-timeStamping).

1.4.2. Utilizările interzise

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 (certificatele de titular nu sunt certificate de autoritate);

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

– pentru activități ilegale.

Utilizarea în afara acestor limite nu este acoperită de răspunderea CERTDIGITAL (secțiunea 9.6). Certificatele nu conțin limite de valoare a tranzacțiilor.

1.4.3. Certificatele de test

CERTDIGITAL permite terților să verifice și să testeze toate tipurile de certificate pe care le emite (ETSI EN 319 411-1, OVR-6.9.2-01). Certificatele din mediul de producție folosite pentru teste respectă politica aplicabilă, inclusiv secțiunea 3.1.3, se folosesc numai pentru documente de test și se revocă la încheierea testului (OVR-6.9.2-01B și -01C). Testele generatorului de certificate și ale aplicațiilor se fac într-o ierarhie de test separată, generată pe o partiție HSM dedicată (alta decât ROOTG5, CAG5 și SVG5), cu subiecte care conțin cuvântul „TEST”; certificatele acestei ierarhii nu sunt calificate și nu se înscriu în Lista de încredere.

1.5. Administrarea politicii

1.5.1. Organizația care administrează documentul

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.

1.5.2. Persoana de contact

– telefon: +40 253 214 767; e-mail: office@certdigital.ro; https://www.certdigital.ro/;

– revocarea certificatelor (24/7): prin portalul client, precum și prin e-mail sau prin cerere scrisă depusă la sediu (secțiunea 4.9.3);

– protecția datelor: dpo@centruldecalcul.ro;

– notificarea incidentelor de securitate: ofițerul de securitate IT, conform documentului „Datele de contact” (00i).

1.5.3. Persoana care stabilește conformitatea DPC cu politica

Conformitatea prezentei DPC cu politicile de certificare și cu cerințele legale este verificată de ofițerul de securitate IT și aprobată de Directorul General al CENTRUL DE CALCUL S.A.

1.5.4. Procedura de aprobare a DPC

Proiectul de DPC este elaborat de echipa CertDigital, verificat de ofițerul de securitate IT și aprobat de Directorul General. Versiunea aprobată se publică în depozit. Modificările se fac conform secțiunii 9.12.

1.6. Definiții și acronime

1.6.1. Definiții

– **certificat calificat** — certificatul care îndeplinește cerințele din anexa I (semnătură) sau anexa III (sigiliu) la Regulamentul (UE) nr. 910/2014 și este emis de un prestator de servicii de încredere calificat;

– **certificat de scurtă durată** — certificatul a cărui perioadă de valabilitate, de la notBefore la notAfter, este mai scurtă decât termenul maxim de prelucrare a unei cereri de revocare declarat în prezenta DPC (24 de ore, secțiunea 4.9.5) (ETSI EN 319 411-1, clauza 3.1);

– **cheie de semnare de unică folosință** — cheia de semnare generată, certificată, utilizată și ștearsă pe baza unei singure autorizări a titularului, legată de o singură sesiune de semnare a unuia sau a mai multor documente (ETSI TS 119 431-1, clauza 3.1);

– **date de activare** — datele (PIN, PUK, parole) necesare pentru utilizarea cheii private;

– **dispozitiv calificat de creare a semnăturilor / sigiliilor (QSCD)** — dispozitivul care îndeplinește cerințele din anexa II la Regulamentul (UE) nr. 910/2014 și este certificat conform art. 30;

– **parte care se bazează** — persoana care se bazează pe o identificare electronică sau pe un serviciu de încredere;

– **titular** — persoana căreia i se emite certificatul (secțiunea 1.3.3);

– **CERTDIGITAL KYC** — soluția proprie a CERTDIGITAL de verificare a identității la distanță, prin înregistrare video verificată automat și ulterior de un operator de înregistrare.

1.6.2. Acronime

Acronim	Semnificație
ADR	Autoritatea pentru Digitalizarea României
CA	autoritate de certificare (Certification Authority)
CAB	organism de evaluare a conformității (Conformity Assessment Body)
CRL	listă de certificate revocate (Certificate Revocation List)
DPC	declarația practicilor de certificare
HSM	modul criptografic hardware (Hardware Security Module)
OCSP	protocolul de verificare online a stării certificatelor (Online Certificate Status Protocol)
OID	identificator de obiect (Object Identifier)
PDS	Declarația de informare a PKI (PKI Disclosure Statement, ETSI EN 319 411-1, anexa A), document publicat separat; informațiile ei sunt cuprinse și în Termenii și condițiile pentru certificatele calificate (TC-CERT)
QSCD	dispozitiv calificat de creare a semnăturilor sau sigiliilor electronice
RA	autoritate de înregistrare (Registration Authority)
TSA	autoritate de marcare temporală (Time-Stamping Authority)
UTC	timpul universal coordonat (Coordinated Universal Time)

2. Responsabilitățile privind publicarea și depozitul

2.1. Depozitele

CERTDIGITAL gestionează următoarele puncte de publicare:

Ce se publică	Adresa
Documentele (DPC, politici, PDS, termeni și condiții, contracte-tip)	https://www.certdigital.ro/repository/
PDS-ul (Declarația de informare a PKI), la care trimite declarația QcPDS din certificatele emise de CERTDIGITAL QCA G5	https://www.certdigital.ro/repository/pds/certdigital_pds_ro.pdf (ro) și https://www.certdigital.ro/repository/pds/certdigital_pds_en.pdf (en)
Certificatele autorităților	http://certs.certdigital.ro/certdigital_root_g5.crt și http://certs.certdigital.ro/certdigital_qualified_g5.crt
Listele de certificate revocate	http://crl.certdigital.ro/certdigital_root_g5.crl și http://crl.certdigital.ro/certdigital_qualified_g5.crl
Serviciul OCSP	http://ocsp.g5.certdigital.ro
Registrul public al certificatelor	https://ca.certdigital.ro/registry

2.2. Publicarea informațiilor

CERTDIGITAL publică: prezenta DPC și celelalte documente de la secțiunea 2.1, certificatele autorităților, listele de certificate revocate, informațiile privind statutul calificat și atestarea de conformitate.

CERTDIGITAL ține registrul electronic al certificatelor emise, public și consultabil permanent la https://ca.certdigital.ro/registry (art. 14 din Legea nr. 214/2024). Pentru fiecare certificat, registrul indică: numărul de serie, autoritatea emitentă, politica de certificare, data și ora emiterii și ale expirării, starea și, după caz, data, ora și motivul revocării. Căutarea se face după numărul de serie sau după adresa de e-mail exactă. Registrul nu afișează codul numeric personal. Certificatul complet poate fi descărcat din registru numai cu acordul titularului, exprimat la contractare și revocabil oricând.

2.3. Momentul sau frecvența publicării

– documentele se publică la aprobarea fiecărei versiuni, conform secțiunii 9.12;

– CRL-ul CERTDIGITAL QCA G5 se emite automat cel puțin o dată la 8 ore și imediat după fiecare revocare (secțiunea 4.9.7);

– CRL-ul CERTDIGITAL ROOT CA G5 se emite cel puțin o dată la 6 luni și imediat după revocarea unui certificat de autoritate;

– registrul public al certificatelor se actualizează la emiterea și la revocarea fiecărui certificat.

2.4. Controlul accesului la depozite

Informațiile publicate sunt disponibile gratuit, fără autentificare, numai pentru citire. Modificarea lor este permisă numai personalului autorizat, prin sisteme protejate conform capitolelor 5 și 6.

Disponibilitatea 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; depozitul de documente și site-ul sunt disponibile 24/7, cu o disponibilitate-țintă de 99% pe an. Întreruperile planificate se anunță pe site cu cel puțin 24 de ore înainte. Informațiile privind starea certificatelor sunt gratuite și rămân disponibile și după expirarea certificatelor (art. 24 alin. (4) din Regulamentul eIDAS).

3. Identificarea și autentificarea

3.1. Denumirea

3.1.1. Tipuri de nume

Emitentul și titularul sunt identificați prin nume distinse (DN) X.500, conform IETF RFC 5280 și ETSI EN 319 412-2 (persoane fizice) și EN 319 412-3 (persoane juridice).

Atribut	Semnătură (persoană fizică)	Sigiliu (persoană juridică)
countryName (C)	da	da
stateOrProvinceName (S)	da	da
localityName (L)	da	da
serialNumber	da (secțiunea 3.1.2)	da (secțiunea 3.1.2)
givenName (G), surname (SN)	da	—
organizationName (O)	—	da, denumirea oficială
organizationIdentifier	—	da, de exemplu VATRO-<CUI>
emailAddress (E)	da	da
commonName (CN)	numele și prenumele	denumirea persoanei juridice sau a sigiliului

Extensia subjectAltName conține adresa de e-mail (rfc822Name) și, după caz, un nume principal de utilizator (UPN).

Tabelul și extensia subjectAltName de mai sus privesc certificatele titularilor. Certificatele autorităților G5 și certificatele de serviciu G5 au numele distins C=RO, O=CENTRUL DE CALCUL S.A., OU=CERTDIGITAL, organizationIdentifier=VATRO-2163993, CN=<denumirea certificatului>: CERTDIGITAL ROOT CA G5, CERTDIGITAL QCA G5, CERTDIGITAL OCSP G5, CERTDIGITAL TSA G5, CERTDIGITAL QESVAL SERVICE G5, CERTDIGITAL QPS SERVICE G5, CERTDIGITAL QEARCH SERVICE G5, CERTDIGITAL QLEDGERS SERVICE G5, CERTDIGITAL QREM SERVICE G5, CERTDIGITAL QERDS SERVICE G5 și CERTDIGITAL QEAA SERVICE G5. Ele nu conțin atributele S, L, serialNumber și E; dintre ele, numai CERTDIGITAL QREM SERVICE G5 conține extensia subjectAltName, cu adresa office@rem.certdigital.ro (secțiunea 7.1.2).

3.1.2. Necesitatea ca numele să fie semnificative

Numele din certificat identifică în mod neechivoc titularul.

– **Până la 28.02.2027**, atributul serialNumber conține identificatorul intern atribuit titularului la înregistrare: un cod alfanumeric, același în toate certificatele titularului, care nu conține codul numeric personal sau codul fiscal. Certificatele de sigiliu conțin, în plus, atributul organizationIdentifier, cu codul fiscal („VATRO-” urmat de codul unic de înregistrare, fără prefixul RO, ca în certificatele CERTDIGITAL: VATRO-2163993).

– **De la 01.03.2027**, atributul serialNumber respectă semantica ETSI EN 319 412-1 (cl. 5.1.3 și 5.1.4): pentru persoanele fizice, „PNORO-” urmat de codul numeric personal, sau „PASRO-” / „IDCRO-” urmat de numărul pașaportului ori al cărții de identitate; pentru persoanele juridice, organizationIdentifier „VATRO-” sau „NTRRO-” urmat de codul fiscal sau de numărul de înregistrare. Certificatul conține și declarația semantică corespunzătoare (0.4.0.194121.1.1 sau 0.4.0.194121.1.2).

3.1.3. Anonimatul sau pseudonimul titularilor

CERTDIGITAL nu emite certificate calificate cu pseudonim.

3.1.4. Reguli de interpretare a diferitelor forme de nume

Numele se înscriu cu diacriticele din actul de identitate, în codificarea UTF-8, conform RFC 5280.

3.1.5. Unicitatea numelor

Combinația de atribute din DN, inclusiv serialNumber, este unică pentru fiecare titular în cadrul CERTDIGITAL QCA G5.

3.1.6. Recunoașterea, autentificarea și rolul mărcilor înregistrate

Solicitantul garantează că are dreptul de a folosi denumirile înscrise în certificat. CERTDIGITAL nu verifică drepturile de proprietate intelectuală asupra denumirilor și nu arbitrează litigii privind mărcile.

3.2. Validarea inițială a identității

3.2.1. Metoda de dovedire a deținerii cheii private

Cererea de certificat se transmite sub forma unei cereri PKCS#10 semnate cu cheia privată corespunzătoare; CERTDIGITAL verifică semnătura cererii. Când cheia este generată de CERTDIGITAL în dispozitivul titularului, deținerea cheii rezultă din procesul de generare, documentat în jurnalele RA. Pentru serviciul rQSCD, cheia se generează în dispozitivul calificat la distanță, iar serviciul transmite RA cererea PKCS#10 semnată cu cheia generată, împreună cu dovada autentificării titularului legate de cheie (ETSI TS 119 431-1, pentru cerința REG-6.3.1-01 din ETSI EN 319 411-1). Pentru cheile de unică folosință, cheia se generează în sesiunea de semnare pentru care a fost cerută, cererea PKCS#10 semnată cu această cheie se transmite în aceeași sesiune, iar CA emite certificatul numai pentru cheia generată în sesiunea respectivă (ETSI TS 119 431-1, GEN-6.2.1-08 și GEN-6.2.1-09).

3.2.2. Autentificarea identității organizației

Pentru certificatele de sigiliu, CERTDIGITAL verifică:

– existența și datele persoanei juridice, pe baza certificatului constatator sau a extrasului din Registrul Comerțului (ONRC) ori a documentului echivalent pentru persoanele juridice străine, cu o vechime de cel mult 30 de zile;

– actul constitutiv sau, după caz, împuternicirea care atestă calitatea persoanei care solicită certificatul;

– identitatea reprezentantului legal sau a persoanei împuternicite, prin una dintre metodele de la secțiunea 3.2.3.

3.2.3. Autentificarea identității persoanelor fizice

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**: titularul (sau reprezentantul legal al persoanei juridice) se prezintă în fața unui operator de înregistrare CERTDIGITAL (angajat al societății, desemnat și instruit), la sediul sau la punctele de lucru ale 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, fără operator, 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 de la înregistrare. Soluția este înscrisă de ADR în Lista terților de verificare a identității persoanei la distanță utilizând mijloace video (adresa ADR nr. 2043/06.08.2026), în condițiile Deciziei președintelui ADR nr. 564/2021 (art. 16 alin. (3) lit. d) și e) din Legea nr. 214/2024; art. 24 alin. (1a) lit. (c) din Regulamentul eIDAS). Compararea biometrică a imaginii faciale se face numai cu consimțământul explicit al titularului; titularul care nu își dă consimțământul poate opta pentru metoda de la lit. a);

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, conform secțiunii 3.3 (art. 24 alin. (1a) lit. (b) din Regulamentul eIDAS; art. 16 alin. (3) lit. b) din Legea nr. 214/2024).

Pentru cetățenii români, valabilitatea actului de identitate se verifică prin Platforma națională de interoperabilitate (art. 12 alin. (8) din Legea nr. 214/2024; Legea nr. 242/2022). Metoda de verificare a identității este indicată în certificat prin identificatorul de politică (secțiunea 1.2). Începând cu 19.08.2027, verificarea identității respectă și Regulamentul de punere în aplicare (UE) 2025/1566 (ETSI TS 119 461 V2.1.1).

Pentru fiecare certificat al unei chei de unică folosință din serviciul rQSCD, identitatea titularului se verifică din nou, fără reutilizarea unei verificări anterioare, numai prin una dintre

metodele de la lit. a) sau b), la nivelul extins din ETSI TS 119 461 (ETSI TS 119 431-1, LNK-A.7-01); pentru sigilii se verifică, în plus, existența persoanei juridice și calitatea reprezentantului (secțiunea 3.2.2). Metoda de la lit. c) nu se aplică acestor certificate. Certificatul se emite numai după încheierea verificării cu rezultat pozitiv și în cel mult 24 de ore de la încheierea ei (PDP-rQSCD, secțiunea 12.2.4), iar o verificare nu se folosește pentru mai multe certificate; datele din certificat se confirmă la emitere (ETSI EN 319 411-1, REG-6.3.1-00B, REG-6.3.1-00D și REG-6.3.1-00E). Cheia se leagă, ca și cheile de lungă durată, de mijlocul de identificare electronică al titularului, aplicația CertDigital ID, înregistrată după verificarea identității (PDP-rQSCD, secțiunea 12.3.1).

Documentele și înregistrările utilizate la verificarea identității se păstrează conform secțiunii 5.5. Detaliile operaționale se află în Regulamentul de identificare și solicitare a certificatului (RIS) și în Regulamentul de validare și aprobare a cererii (RVA).

Soluția CERTDIGITAL KYC a fost evaluată de LL-C (Certification) Czech Republic a.s. față de normele ADR și ETSI TS 119 461 V2.1.1 (raport din 09.07.2026, fără neconformități), iar CENTRUL DE CALCUL S.A. este înscrisă în lista ADR a terților de verificare a identității prin mijloace video (adresa ADR nr. 2043/06.08.2026).

3.2.4. Informațiile neverificate ale titularului

Adresa de e-mail se verifică prin trimiterea unui mesaj de confirmare. Nu se înscriu în certificat informații neverificate.

3.2.5. Validarea autorității

Calitatea de reprezentant al persoanei juridice se verifică conform secțiunii 3.2.2. Pentru certificatele solicitate de o persoană juridică pentru angajații săi, se verifică împuternicirea solicitantului și acordul titularului.

3.2.6. Criterii de interoperabilitate

Nu se aplică. CERTDIGITAL nu are acorduri de certificare încrucișată.

3.3. Identificarea și autentificarea pentru reînnoirea cheii

3.3.1. Reînnoirea de rutină a cheii

Reînnoirea unui certificat se face numai cu generarea unei perechi noi de chei. Reînnoirea la distanță, pe baza certificatului calificat CERTDIGITAL valabil, emis după verificarea identității prin prezență fizică sau prin CERTDIGITAL KYC, este permisă o singură dată consecutiv. La reînnoirea următoare, identitatea titularului se verifică din nou prin prezență fizică sau prin CERTDIGITAL KYC.

Cererea de reînnoire la distanță se semnează cu certificatul calificat valabil; datele de identificare se verifică din nou dacă s-au modificat.

Certificatele cheilor de unică folosință din serviciul rQSCD nu se reînnoiesc și nici nu li se schimbă cheia: pentru fiecare sesiune de semnare se generează o cheie nouă și se emite un certificat nou, după o nouă verificare a identității (secțiunea 3.2.3).

3.3.2. Reînnoirea cheii după revocare

După revocare, emiterea unui certificat nou urmează procedura de validare inițială (secțiunea 3.2).

3.4. Identificarea și autentificarea pentru cererea de revocare

Cererea de revocare se poate face:

– prin portalul client, după autentificarea titularului;

– prin e-mail semnat cu un certificat calificat sau prin cerere scrisă depusă la sediu, cu verificarea identității solicitantului;

– de către CERTDIGITAL, din oficiu, în cazurile de la secțiunea 4.9.1.

Identitatea și dreptul solicitantului de a cere revocarea se verifică conform procedurii interne de revocare. Dacă verificarea nu poate fi finalizată, dar există indicii de compromitere a cheii, CERTDIGITAL revocă certificatul și informează titularul.

4. Cerințe operaționale privind ciclul de viață al certificatelor

4.1. Cererea de certificat

4.1.1. Cine poate depune o cerere

– persoana fizică, pentru propriul certificat de semnătură;

– persoana juridică, prin reprezentantul legal sau printr-o persoană împuternicită, pentru certificatul de sigiliu;

– persoana juridică, pentru certificatele de semnătură ale angajaților sau reprezentanților săi, cu acordul fiecărui titular, exprimat la verificarea identității.

4.1.2. Procesul de înregistrare și responsabilitățile

Solicitantul completează cererea (în portalul client sau la ghișeu), acceptă termenii și condițiile și semnează contractul. Înainte de încheierea contractului, CERTDIGITAL pune la dispoziția solicitantului termenii și condițiile, PDS-ul (Declarația de informare a PKI) și prezenta DPC (art. 24 alin. (2) lit. (d) din Regulamentul eIDAS). Clauzele privind limitările de utilizare, răspunderea și soluționarea litigiilor se acceptă în mod expres.

Solicitantul răspunde de exactitatea datelor furnizate și informează CERTDIGITAL despre orice modificare a acestora.

4.2. Prelucrarea cererii

4.2.1. Efectuarea identificării și autentificării

Operatorul de înregistrare verifică identitatea conform secțiunii 3.2 și conformitatea datelor din cerere cu documentele prezentate.

4.2.2. Aprobarea sau respingerea cererii

Cererea este aprobată de operatorul de înregistrare dacă toate verificările sunt îndeplinite. Cererea se respinge dacă identitatea nu poate fi verificată, dacă documentele sunt incomplete, expirate sau suspecte ori dacă solicitantul nu acceptă termenii și condițiile. Solicitantul este informat cu privire la respingere.

4.2.3. Durata de prelucrare a cererii

Certificatul se emite în cel mult 5 zile lucrătoare de la verificarea identității, dacă cererea este completă. Pentru identificarea prin CERTDIGITAL KYC, verificarea înregistrării de către operator se face în cel mult 24 de ore. Termenul de cel mult 5 zile lucrătoare nu se aplică certificatelor cheilor de unică folosință, care se emit în sesiunea de semnare, imediat după generarea cheii, în condițiile secțiunii 3.2.3.

4.3. Emiterea certificatului

4.3.1. Acțiunile CA în timpul emiterii

După aprobare, cererea este semnată de operatorul de înregistrare și transmisă către CERTDIGITAL QCA G5, care emite certificatul. Emiterea se face într-un mediu securizat, cu cheia CA păstrată în modulul criptografic hardware (secțiunea 6.2). Data de început a valabilității este data emiterii; nu se emit certificate cu valabilitate în trecut sau în viitor. Pentru cheile de unică folosință, cererea se transmite automat de serviciul rQSCD, în sesiunea de semnare, pe baza verificării identității aprobate de operatorul de înregistrare pentru acel certificat (secțiunea 3.2.3); certificatul de scurtă durată are data de început egală cu momentul emiterii, fără antedatare, și o valabilitate de cel mult 60 de minute (secțiunea 6.3.2).

CERTDIGITAL ROOT CA G5 emite numai certificatul CERTDIGITAL QCA G5, în ceremonia de generare a cheilor (secțiunea 6.1.1). Certificatele de serviciu G5 se emit de CERTDIGITAL QCA G5 în aceeași ceremonie, pe baza profilurilor aprobate (secțiunea 7.1), iar fiecare certificat se verifică înainte de emiterea celui următor. Rezultatele se consemnează în procesul-verbal al ceremoniei.

4.3.2. Notificarea titularului

Titularul este informat prin e-mail despre emitere. Certificatul se transmite pe un canal securizat (art. 11 alin. (4) din Legea nr. 214/2024): instalat în dispozitivul criptografic livrat titularului sau descărcat de titular prin aplicațiile CertDigital, după autentificare.

4.4. Acceptarea certificatului

4.4.1. Modul de acceptare

Certificatul se consideră acceptat de titular la prima sa utilizare sau, în lipsa unei obiecții transmise CERTDIGITAL, la împlinirea a 7 zile calendaristice de la punerea sa la dispoziție, oricare dintre aceste momente intervine primul. Certificatul unei chei de unică folosință se consideră acceptat la prima sa utilizare, în sesiunea de semnare în care a fost emis; termenul de 7 zile nu se aplică acestor certificate. Certificatul CERTDIGITAL QCA G5 și certificatele de serviciu G5 se consideră acceptate la semnarea procesului-verbal al ceremoniei, după verificarea conținutului lor.

4.4.2. Publicarea certificatului de către CA

După acceptare, certificatul se înscrie în registrul public al certificatelor (secțiunea 2.2), cu datele prevăzute la art. 14 din Legea nr. 214/2024. Certificatul complet poate fi descărcat din registru numai cu acordul titularului. Certificatele autorităților se publică în depozit (secțiunea

2.1); pentru certificatul CERTDIGITAL QCA G5 și pentru certificatele de serviciu care identifică servicii calificate, CERTDIGITAL solicită ADR înscrierea în Lista de încredere.

4.4.3. Notificarea altor entități

La emiterea certificatului CERTDIGITAL QCA G5 și a certificatelor de serviciu G5, ADR și organismul de evaluare a conformității sunt informați, conform Procedurii de notificare (00q). Pentru celelalte certificate nu se aplică.

4.5. Utilizarea perechii de chei și a certificatului

4.5.1. Utilizarea cheii private și a certificatului de către titular

Titularul:

– utilizează cheia privată numai în scopurile de la secțiunea 1.4.1 și numai în dispozitivul în care a fost generată;

– păstrează sub control exclusiv dispozitivul și datele de activare și nu le dezvăluie altor persoane (art. 26 din Legea nr. 214/2024);

– solicită revocarea 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;

– încetează utilizarea cheii după expirarea sau revocarea certificatului.

4.5.2. Utilizarea cheii publice și a certificatului de către partea care se bazează

Partea care se bazează:

– verifică validitatea semnăturii sau a sigiliului și lanțul de certificare până la CERTDIGITAL ROOT CA G5;

– verifică starea certificatului la momentul relevant, prin OCSP sau CRL;

– pentru semnăturile și sigiliile create cu certificatele de scurtă durată ale cheilor de unică folosință, stabilește momentul creării lor pe baza mărcii temporale calificate din semnătură, aplicate în perioada de valabilitate a certificatului (nivelul B-T sau superior);

– respectă limitările de utilizare din certificat și din prezenta DPC;

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

4.6. Reînnoirea certificatului (fără schimbarea cheii)

4.6.1. Circumstanțele reînnoirii

Nu se aplică. CERTDIGITAL nu emite certificate noi pentru o cheie publică existentă; reînnoirea se face numai cu o pereche nouă de chei (secțiunea 4.7).

4.6.2. Cine poate solicita reînnoirea

Nu se aplică.

4.6.3. Prelucrarea cererii de reînnoire

Nu se aplică.

4.6.4. Notificarea titularului

Nu se aplică.

4.6.5. Modul de acceptare

Nu se aplică.

4.6.6. Publicarea certificatului reînnoit

Nu se aplică.

4.6.7. Notificarea altor entități

Nu se aplică.

4.7. Reînnoirea cu schimbarea cheii

4.7.1. Circumstanțele

Titularul poate solicita un certificat nou, cu o pereche nouă de chei, înainte de expirarea certificatului existent sau după expirarea ori revocarea acestuia. Certificatele cheilor de unică folosință nu se reînnoiesc (secțiunea 3.3.1).

4.7.2. Cine poate solicita

Titularul sau solicitantul care a obținut certificatul inițial.

4.7.3. Prelucrarea cererii

Identitatea se verifică conform secțiunii 3.3. Reînnoirea la distanță pe baza certificatului calificat valabil este permisă o singură dată consecutiv; certificatul nou emis astfel conține codul de identificare 6 în identificatorul de politică (secțiunea 1.2).

4.7.4. Notificarea titularului

Conform secțiunii 4.3.2.

4.7.5. Modul de acceptare

Conform secțiunii 4.4.1.

4.7.6. Publicarea certificatului

Conform secțiunii 4.4.2.

4.7.7. Notificarea altor entități

Nu se aplică.

4.8. Modificarea certificatului

4.8.1. Circumstanțele

Certificatele emise nu se modifică. Dacă datele titularului se schimbă, certificatul se revocă și, la cerere, se emite un certificat nou, după verificarea identității.

4.8.2. Cine poate solicita modificarea

Nu se aplică.

4.8.3. Prelucrarea cererii

Nu se aplică.

4.8.4. Notificarea titularului

Nu se aplică.

4.8.5. Modul de acceptare

Nu se aplică.

4.8.6. Publicarea certificatului modificat

Nu se aplică.

4.8.7. Notificarea altor entități

Nu se aplică.

4.9. Revocarea și suspendarea certificatului

4.9.1. Circumstanțele revocării

Certificatul se revocă, în cel mult 24 de ore de la luarea la cunoștință (art. 17 alin. (2) din Legea nr. 214/2024), în special când:

– titularul sau solicitantul cere revocarea;

– cheia privată sau datele de activare sunt pierdute, compromise ori există suspiciunea compromiterii;

– datele din certificat sunt false sau nu mai corespund realității;

– titularul persoană fizică a decedat sau titularul persoană juridică și-a încetat existența;

– certificatul este utilizat în mod fraudulos sau cu încălcarea termenilor și condițiilor;

– există un posibil incident de securitate care afectează certificatul;

– revocarea este dispusă prin hotărâre judecătorească sau cerută de ADR;

– titularul nu își respectă obligațiile contractuale esențiale;

– cheia CERTDIGITAL QCA G5 este compromisă sau CERTDIGITAL încetează serviciul fără preluare;

– în alte cazuri prevăzute de lege sau de prezenta DPC.

Certificatul CERTDIGITAL QCA G5 se revocă de CERTDIGITAL ROOT CA G5, într-o ceremonie, sub control multipersoană și cu proces-verbal, atunci când cheia privată a autorității subordonate este compromisă sau există suspiciunea compromiterii, când autoritatea își încetează activitatea fără preluare, când datele din certificat nu mai sunt corecte, când revocarea este dispusă prin hotărâre judecătorească sau cerută de ADR ori când certificatul a fost emis cu încălcarea prezentei DPC (secțiunile 5.7.3 și 5.8). CRL-ul autorității rădăcină se emite imediat după revocare și se publică în cel mult 24 de ore de la luarea la cunoștință a motivului de revocare. Certificatele de serviciu G5 se revocă de CERTDIGITAL QCA G5 în aceleași condiții ca certificatele titularilor, precum și la înlocuirea cheii serviciului.

4.9.2. Cine poate solicita revocarea

Titularul; solicitantul care a obținut certificatul (de exemplu angajatorul, pentru certificatele angajaților); reprezentantul legal al persoanei juridice titulare; instanța sau ADR; CERTDIGITAL, din oficiu. Revocarea certificatului CERTDIGITAL QCA G5 sau a unui certificat de serviciu G5 poate fi cerută de Directorul General al CENTRUL DE CALCUL S.A., de ofițerul de securitate IT, de instanță sau de ADR.

4.9.3. Procedura de revocare

Cererea se transmite:

– 24/7, prin portalul client, după autentificare;

– prin e-mail semnat electronic calificat sau prin cerere scrisă depusă la sediu, în programul de lucru.

Cererea de revocare se procesează în cel mult 24 de ore de la primire sau de la data la care CERTDIGITAL a luat cunoștință de un motiv de revocare. Revocarea se publică imediat prin serviciul OCSP și se include în CRL-ul emis imediat după înregistrarea revocării (secțiunea 4.9.7). Titularul este informat de îndată, cu indicarea motivelor și a dreptului de a solicita verificarea deciziei. Revocarea este definitivă și devine opozabilă terților de la data înscrierii în registrul certificatelor.

Pentru certificatele din serviciul rQSCD, revocarea este urmată de distrugerea cheii și a copiilor ei de rezervă. Independent de revocare, activarea cheii poate fi blocată imediat, 24/7, la cererea titularului sau din oficiu, fără suspendarea certificatului (PDP-rQSCD, secțiunea 6.9).

Certificatele de scurtă durată ale cheilor de unică folosință sunt revocabile, ca celelalte certificate emise de CERTDIGITAL QCA G5: revocarea se poate cere de persoanele de la secțiunea 4.9.2, prin canalele de mai sus, sau se dispune de CERTDIGITAL, din oficiu, în cazurile de la secțiunea 4.9.1; cererea primită în perioada de valabilitate se prelucrează în termenul de la secțiunea 4.9.5 și se publică în CRL și OCSP și dacă certificatul a expirat între timp (secțiunea 4.10.1). Niciun certificat de scurtă durată emis conform prezentei DPC nu este exceptat de la revocare, nici prin serviciul de revocare, nici din oficiu, și niciunul nu conține extensia „validity assured” pentru certificatele de scurtă durată (ETSI EN 319 411-1, REV-6.3.9-15A, REV-6.3.9-16 și GEN-6.6.1-04). Cheia de unică folosință se șterge la încheierea sesiunii de semnare fără revocarea certificatului: ștergerea cheii nu este o revocare (ETSI TS 119 431-1, clauza 4, nota 2), iar semnăturile create în sesiune rămân valabile. Dacă certificatul se revocă înainte de încheierea sesiunii, cheia se șterge imediat și sesiunea se închide.

4.9.4. Perioada de grație pentru cererea de revocare

Nu există perioadă de grație. Titularul solicită revocarea în cel mult 24 de ore de la apariția motivului (art. 26 din Legea nr. 214/2024).

4.9.5. Termenul în care CA trebuie să prelucreze cererea

Cel mult 24 de ore de la primirea cererii sau de la luarea la cunoștință (art. 24 alin. (3) din Regulamentul eIDAS; art. 17 alin. (2) din Legea nr. 214/2024).

4.9.6. Cerințe de verificare a revocării pentru părțile care se bazează

Partea care se bazează verifică starea certificatului prin OCSP sau prin cea mai recentă CRL, conform secțiunii 4.5.2. Pentru certificatul autorității subordonate, partea care se bazează verifică cea mai recentă CRL a autorității rădăcină.

4.9.7. Frecvența emiterii CRL

CRL-ul CERTDIGITAL QCA G5 se emite automat cel puțin o dată la 8 ore și imediat după fiecare revocare, cu o perioadă de valabilitate (nextUpdate) de 24 de ore. CRL-ul CERTDIGITAL ROOT CA G5 se emite cel puțin o dată la 6 luni, cu valabilitate de un an, și imediat după revocarea unui certificat de autoritate. CRL-urile nu se lasă să expire: un CRL nou se emite înaintea datei nextUpdate a celui în vigoare. Numărul CRL (cRLNumber) crește la fiecare emitere, separat pentru fiecare autoritate, și nu se reutilizează (IETF RFC 5280, secțiunea 5.2.3).

4.9.8. Latența maximă a CRL

CRL-ul se publică în depozit imediat după emitere.

4.9.9. Disponibilitatea verificării online a stării

Serviciul OCSP (http://ocsp.g5.certdigital.ro), conform IETF RFC 6960, este disponibil 24/7, cu o disponibilitate-țintă de 99,5% pe an, și acceptă cereri prin HTTP, cu metodele POST și GET (IETF RFC 6960, anexa A.1). Răspunsurile sunt semnate de responderul autorizat de CERTDIGITAL QCA G5, cu certificatul CERTDIGITAL OCSP G5, emis de aceasta, valabil 3 ani, care conține extensia id-pkix-ocsp-nocheck (IETF RFC 6960, secțiunea 4.2.2.2; secțiunea 7.3). Certificatul CERTDIGITAL QCA G5 nu indică un serviciu OCSP în extensia authorityInfoAccess, iar starea lui se verifică prin CRL-ul autorității rădăcină. Starea unei revocări este disponibilă prin OCSP imediat după înregistrarea acesteia.

4.9.10. Cerințe pentru verificarea online

Nu există cerințe suplimentare față de secțiunea 4.9.6. Revocarea apare în OCSP imediat după înregistrare, iar în CRL la emiterea care urmează imediat revocării (secțiunea 4.9.7). Pentru ambele metode, schimbarea stării este disponibilă în cel mult 24 de ore de la primirea cererii de revocare (ETSI EN 319 411-1, REV-6.2.4-03A și REV-6.2.4-03C). Dacă, pentru scurt timp, răspunsul OCSP și CRL-ul diferă, prevalează informația cea mai recentă. Revocarea este definitivă (secțiunea 4.9.13), astfel încât un certificat indicat ca revocat de oricare dintre cele două surse se consideră revocat de la data revocării (ETSI EN 319 411-1, CSS-6.3.10-09A).

4.9.11. Alte forme de anunțare a revocării

La revocarea certificatului CERTDIGITAL QCA G5 sau a unui certificat de serviciu G5 care identifică un serviciu calificat, CERTDIGITAL publică un anunț pe site și solicită ADR actualizarea Listei de încredere. Pentru celelalte certificate nu se aplică.

4.9.12. Cerințe speciale privind compromiterea cheii

La compromiterea sau suspiciunea compromiterii cheii private, titularul încetează imediat utilizarea cheii și solicită revocarea. La compromiterea cheii CERTDIGITAL QCA G5 se aplică secțiunea 5.7.3.

4.9.13. Circumstanțele suspendării

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 în cel mult 24 de ore. Titularul este informat în prealabil că revocarea este definitivă. Dacă motivul încetează, la cerere, CERTDIGITAL emite un certificat nou, după verificarea identității, fără costuri suplimentare.

4.9.14. Cine poate solicita suspendarea

Nu se aplică.

4.9.15. Procedura de suspendare

Nu se aplică.

4.9.16. Limitele perioadei de suspendare

Nu se aplică.

4.10. Serviciile privind starea certificatelor

4.10.1. Caracteristici operaționale

Starea certificatelor este disponibilă prin CRL (secțiunea 4.9.7) și OCSP (secțiunea 4.9.9). Certificatele revocate rămân în CRL și după expirarea lor, iar serviciul OCSP furnizează starea și pentru certificatele expirate (art. 24 alin. (4) din Regulamentul eIDAS). Starea certificatelor de autoritate este disponibilă prin CRL-ul autorității rădăcină, inclusiv după expirarea lor. Starea certificatelor de scurtă durată ale cheilor de unică folosință se publică la fel, prin CRL și OCSP, pe durata valabilității și după expirarea lor (ETSI EN 319 411-2, CSS-6.3.10-02); CERTDIGITAL nu folosește pentru ele excepția de la serviciile de stare prevăzută pentru certificatele de scurtă durată cu valabilitate asigurată (ETSI EN 319 411-2, CSS-6.3.10-02A).

CRL-urile CERTDIGITAL QCA G5 și CERTDIGITAL ROOT CA G5 conțin extensia ExpiredCertsOnCRL (OID 2.5.29.60, ITU-T X.509), cu data de început a valabilității certificatului autorității emitente, care arată că certificatele revocate rămân în CRL și după expirare (ETSI EN 319 411-2, CSS-6.3.10-05). Răspunsurile OCSP conțin extensia archiveCutoff (IETF RFC 6960, secțiunea 4.4.4), cu aceeași dată (ETSI EN 319 411-2, CSS-6.3.10-10).

Informațiile privind starea certificatelor sunt disponibile pe toată durata de funcționare a autorității emitente și după încetarea acesteia, conform secțiunii 5.8. La compromiterea cheii CERTDIGITAL QCA G5, revocarea certificatului acesteia se publică în CRL-ul autorității rădăcină; la compromiterea cheii autorității rădăcină, situația ierarhiei se comunică prin Lista de încredere și prin anunțul de pe site (secțiunile 4.9.11 și 5.7.3; ETSI EN 319 411-2, CSS-6.3.10-12).

4.10.2. Disponibilitatea serviciului

OCSP și CRL: 24/7, cu disponibilitate-țintă de 99,5% pe an. CERTDIGITAL face tot posibilul ca o întrerupere neplanificată să nu depășească 4 ore (RTO, secțiunea 5.7.4; ETSI EN 319 411-1, CSS-6.3.10-02). Întreruperile planificate se anunță pe site cu cel puțin 24 de ore înainte.

4.10.3. Caracteristici opționale

Nu se aplică.

4.11. Încetarea contractului

Contractul încetează la expirarea sau revocarea ultimului certificat al titularului ori prin acordul părților. Încetarea nu afectează obligațiile de păstrare a înregistrărilor (secțiunea 5.5).

4.12. Păstrarea în custodie și recuperarea cheilor

4.12.1. Politica și practicile de custodie și recuperare a cheilor

Pentru certificatele pe dispozitivul titularului, CERTDIGITAL nu păstrează, nu arhivează și nu poate recupera cheile private; cheile se generează și rămân exclusiv în dispozitivul titularului.

Pentru serviciul rQSCD, cheile se generează și se păstrează de CERTDIGITAL în dispozitivul calificat la distanță, în numele titularului și sub controlul exclusiv al acestuia. Ele se duplică numai pentru copii de rezervă, în condițiile art. 29a alin. (1) lit. (b) din Regulamentul eIDAS (secțiunea 6.2.4), nu se predau titularului sau terților și nu se recuperează în afara dispozitivului. O cheie de unică folosință există numai în baza de date a dispozitivului și în replica ei din centrul de date secundar, pe durata sesiunii de semnare de care este legată, și se șterge din ambele imediat după încheierea sesiunii; copiile de rezervă ale bazei de date care ar mai conține-o, în formă criptată, nu pot fi restaurate fără reaplicarea ștergerilor, astfel încât cheia nu mai poate fi activată (ETSI TS 119 431-1, DEL-6.3.2-04 și DEL-6.3.2-05; PDP-rQSCD, secțiunile 6.7 și 13.4).

4.12.2. Politica și practicile de încapsulare și recuperare a cheilor de sesiune

Nu se aplică.

5. Controale privind facilitățile, managementul și operarea

5.1. Controale fizice

5.1.1. Amplasarea și construcția

Infrastructura serviciilor de încredere este găzduită în două centre de date proprii din Târgu Jiu, aflate în clădiri separate: un centru principal și un centru secundar de rezervă, pregătit să preia serviciile (activ-pasiv), inclusiv cu modul criptografic (HSM). Centrul principal este proiectat după recomandările TIA-942 pentru nivelul Tier 3. Accesul fizic este controlat pe zone de securitate, cu autentificare în patru factori (cheie, cartelă, cod și amprentă, în această ordine). Măsurile detaliate de protecție sunt descrise în documentația internă de securitate și sunt puse la dispoziția organismului de evaluare a conformității și a organismului de supraveghere.

5.1.2. Accesul fizic

Echipamentele CA, HSM-urile și componentele critice sunt amplasate în zona de securitate cea mai restrictivă. Accesul este permis numai persoanelor cu roluri de încredere autorizate, este înregistrat electronic și supravegheat video. Vizitatorii au acces numai însoțiți, pe baza unui registru de acces.

5.1.3. Alimentarea cu energie și climatizarea

Centrele de date au alimentare electrică redundantă, surse neîntreruptibile (UPS) și generator, precum și climatizare redundantă, dimensionate pentru funcționarea continuă a serviciilor.

5.1.4. Expunerea la apă

Echipamentele sunt amplasate în spații protejate împotriva inundațiilor: sunt montate în rafturi la cel puțin 15 cm deasupra pardoselii, iar camerele de date sunt monitorizate cu senzori de umiditate și de inundație.

5.1.5. Prevenirea și protecția împotriva incendiilor

Centrele de date au sisteme de detecție și alarmare la incendiu și mijloace de stingere adecvate echipamentelor electronice.

5.1.6. Păstrarea suporturilor de stocare

Suporturile care conțin date sensibile (copii de siguranță, arhive, plicurile sigilate cu datele de activare ale HSM) se păstrează în spații securizate, cu acces controlat, protejate împotriva deteriorării și a accesului neautorizat.

5.1.7. Eliminarea deșeurilor

Suporturile care au conținut date sensibile se distrug sau se șterg securizat înainte de eliminare, cu înregistrarea operației.

5.1.8. Copiile de rezervă în afara locației

Copiile de siguranță se păstrează în centrul de date secundar, iar o copie suplimentară se păstrează offline, separat de ambele centre de date. Cheile autorităților de certificare nu se includ în copiile de siguranță; ele sunt protejate conform secțiunii 6.2.4.

5.2. Controale procedurale

5.2.1. Rolurile de încredere

Rolurile de încredere sunt atribuite exclusiv angajaților CENTRUL DE CALCUL S.A., numiți prin decizie a Directorului General:

– **ofițerul de securitate IT** — răspunde de implementarea politicilor de securitate și de notificarea incidentelor;

– **administratorii de sistem** — instalează, configurează și întreține sistemele CA, RA, OCSP și infrastructura;

– **operatorii de sistem** — operează zilnic sistemele, inclusiv copiile de siguranță și recuperarea;

– **operatorii de înregistrare** — verifică identitatea și aprobă cererile de certificat și de revocare;

– **auditorii de sistem** — au acces numai pentru citire la jurnale și arhive;

– **custozii HSM** — dețin componentele secrete (componentele parolelor modulului și ale partițiilor) necesare activării și administrării HSM.

Persoanele cu roluri de încredere nu au conflicte de interese care să le afecteze imparțialitatea și au semnat angajamente de confidențialitate.

5.2.2. Numărul de persoane necesare pentru fiecare activitate

Operațiile cu cheile autorităților (generare, activare, copiere de rezervă, restaurare, distrugere) și administrarea HSM se efectuează sub control dual sau multiplu (M din N), în prezența a cel puțin două persoane cu roluri de încredere diferite. Situațiile concrete sunt descrise în Procedura privind generarea cheilor (document intern).

5.2.3. Identificarea și autentificarea pentru fiecare rol

Fiecare persoană cu rol de încredere are un cont nominal, nepartajat, cu drepturi limitate la rolul său, și se autentifică prin cel puțin doi factori. Acțiunile sunt jurnalizate și pot fi atribuite persoanei care le-a efectuat.

5.2.4. Rolurile care necesită separarea sarcinilor

Rolurile de ofițer de securitate, administrator de sistem, operator de înregistrare și auditor de sistem sunt separate: aceeași persoană nu poate deține simultan două dintre aceste roluri pentru aceleași sisteme.

5.3. Controale privind personalul

5.3.1. Calificări, experiență și autorizări

Personalul cu roluri de încredere are calificarea și experiența necesare rolului, verificate la angajare (CV, diplome, referințe), conform ETSI EN 319 401, cl. 7.2.

5.3.2. Verificarea antecedentelor

Înainte de atribuirea unui rol de încredere se verifică cazierul judiciar, în condițiile legii. Verificarea se repetă la cel mult 3 ani.

5.3.3. Instruirea

Personalul este instruit, la numire și ori de câte ori este necesar, privind: prezenta DPC și procedurile aplicabile, securitatea informației, protecția datelor cu caracter personal, verificarea identității și a documentelor, gestionarea incidentelor. Instruirea se documentează.

5.3.4. Frecvența reinstruirii

Reinstruirea are loc cel puțin anual și la orice modificare semnificativă a sistemelor sau a procedurilor.

5.3.5. Rotația posturilor

Nu se aplică o rotație obligatorie; continuitatea rolurilor este asigurată prin înlocuitori desemnați.

5.3.6. Sancțiuni pentru acțiuni neautorizate

Acțiunile neautorizate sau încălcarea procedurilor se sancționează disciplinar, conform Codului muncii și regulamentului intern, fără a aduce atingere răspunderii civile sau penale.

5.3.7. Cerințe pentru personalul extern

Personalul furnizorilor are acces la sisteme numai însoțit de personal autorizat, pe baza unui contract cu clauze de confidențialitate, și nu îndeplinește roluri de încredere.

5.3.8. Documentația pusă la dispoziția personalului

Personalul are acces la prezenta DPC, la politicile de certificare, la procedurile interne și la manualele aplicațiilor necesare rolului său.

5.4. Procedurile de jurnalizare pentru audit

5.4.1. Tipurile de evenimente înregistrate

Se înregistrează, cu data și ora:

– evenimentele privind ciclul de viață al cheilor autorităților și ale HSM;

– cererile de certificat, verificările de identitate, aprobările și respingerile;

– emiterea, acceptarea și revocarea certificatelor, emiterea CRL-urilor;

– pentru serviciul rQSCD, generarea, legarea certificatului, activarea și ștergerea cheilor semnatarilor, iar pentru cheile de unică folosință și sesiunea de semnare de care este legată fiecare cheie, verificarea identității pe care se bazează certificatul și certificatul emis (CEN EN 419 241-1, SRG_AA.1.1; PDP-rQSCD, secțiunea 14.5);

– accesul la sisteme, autentificările reușite și eșuate, modificările de configurație și de drepturi;

– accesul fizic în zonele de securitate;

– incidentele de securitate și alarmele.

5.4.2. Frecvența prelucrării jurnalelor

Jurnalele se colectează în sistemul centralizat de jurnalizare și se analizează zilnic, automat, cu alertare la evenimente anormale; analiza manuală se face cel puțin lunar.

5.4.3. Perioada de păstrare a jurnalelor

Jurnalele de audit se păstrează cel puțin 10 ani (secțiunea 5.5.2).

5.4.4. Protecția jurnalelor

Jurnalele sunt protejate împotriva modificării și ștergerii neautorizate; accesul la ele este limitat la ofițerul de securitate, la auditorii de sistem și la evaluatori.

5.4.5. Copiile de rezervă ale jurnalelor

Jurnalele se includ în copiile de siguranță (secțiunea 5.1.8).

5.4.6. Sistemul de colectare

Intern, centralizat.

5.4.7. Notificarea persoanei care a generat evenimentul

Nu se aplică.

5.4.8. Evaluarea vulnerabilităților

Se efectuează scanări de vulnerabilitate trimestriale, cu raport, și un test de penetrare anual, efectuat de un terț independent pe toate punctele de acces (măsura M-08 din GR-TSP), precum și analiza de risc anuală, conform ETSI EN 319 401 și cerințelor NIS2.

5.5. Arhivarea înregistrărilor

5.5.1. Tipurile de înregistrări arhivate

Certificatele emise, CRL-urile, cererile și contractele, documentele și datele utilizate la verificarea identității (inclusiv înregistrările video realizate prin CERTDIGITAL KYC), cererile și deciziile de revocare, jurnalele de audit, versiunile documentelor publicate și rapoartele de evaluare.

5.5.2. Perioada de păstrare

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 pentru o perioadă de cel puțin 10 ani de la încetarea valabilității certificatului (expirare sau revocare). În caz de încetare a activității, înregistrările sunt păstrate și puse la dispoziție conform Planului de încetare (art. 16 alin. (2) din Legea nr. 214/2024; Ord. MEDAT nr. 102/2026, cap. IV; art. 24 alin. (2) lit. (h) din Regulamentul eIDAS).

5.5.3. Protecția arhivei

Arhiva este protejată împotriva accesului neautorizat, modificării, ștergerii și deteriorării; integritatea se verifică periodic.

5.5.4. Copiile de rezervă ale arhivei

Conform secțiunii 5.1.8.

5.5.5. Marcarea temporală a înregistrărilor

Toate sistemele sunt sincronizate cu sursa de timp UTC a CERTDIGITAL (secțiunea 6.8); înregistrările conțin data și ora UTC.

5.5.6. Sistemul de colectare a arhivei

Intern.

5.5.7. Proceduri de obținere și verificare a informațiilor din arhivă

Informațiile din arhivă sunt accesibile personalului autorizat, evaluatorilor și autorităților, în condițiile legii. Titularul poate obține informațiile care îl privesc, conform secțiunii 9.4.

5.6. Schimbarea cheii autorității

Cheile CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5 nu se utilizează pentru emiterea de certificate a căror valabilitate ar depăși data expirării certificatului autorității emitente (25, respectiv 15 ani de la ceremonia de generare a cheii). Înaintea acestei date, CERTDIGITAL generează o pereche nouă de chei pentru o autoritate nouă, într-o ceremonie documentată, și informează ADR cu cel puțin o lună înainte. Cheia veche continuă să semneze CRL-uri până la expirarea ultimului certificat emis.

Certificatele de serviciu G5 (CERTDIGITAL OCSP G5 și CERTDIGITAL TSA G5, valabile 3 ani; certificatele celorlalte servicii, valabile 5 ani) se înlocuiesc înainte de expirare, cu chei noi, generate în ceremonie (certificatul CERTDIGITAL TSA G5, cel târziu la încheierea perioadei de utilizare a cheii, de cel mult 2 ani, secțiunea 6.3.2); ADR este informată conform Procedurii de notificare (00q, cap. 12), pentru actualizarea Listei de încredere.

5.7. Compromiterea și recuperarea în caz de dezastru

5.7.1. Gestionarea incidentelor și a compromiterii

CERTDIGITAL aplică o procedură de gestionare și notificare a incidentelor de securitate (Procedura de notificare a incidentelor, 00q). Orice încălcare a securității sau pierdere a integrității cu impact semnificativ asupra serviciilor de încredere ori asupra datelor cu caracter personal se notifică, fără întârzieri nejustificate:

– **Autorității pentru Digitalizarea României**, în cel mult 24 de ore de la luarea la cunoștință (art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS);

– **Directoratului Național de Securitate Cibernetică**: avertizare timpurie în cel mult 24 de ore, notificare în cel mult 72 de ore și raport final în cel mult o lună (OUG nr. 155/2024; CENTRUL DE CALCUL S.A. este înscrisă în Registrul Entităților ca entitate esențială, nr. E-210D02);

– **Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal**, în cel mult 72 de ore, dacă sunt afectate date cu caracter personal (art. 33 GDPR);

– **persoanelor afectate**, fără întârzieri nejustificate, dacă incidentul le poate afecta (art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS; art. 34 GDPR);

– publicului sau altor autorități, la cererea ADR.

Incidentele se înregistrează într-un registru păstrat 10 ani.

5.7.2. Coruperea resurselor, a programelor sau a datelor

Sistemele se restaurează din copiile de siguranță sau prin activarea centrului de date secundar, conform Procedurii de continuitate operațională și de recuperare în caz de dezastru (PO/SI/63). Înainte de reluarea emiterii se verifică integritatea bazei de date CA și a jurnalelor, iar cererile de revocare primite în ultimul interval de replicare se reconciliază și se reprocesează.

5.7.3. Compromiterea cheii private a autorității

La compromiterea sau suspiciunea de compromitere a cheii private CERTDIGITAL QCA G5, CERTDIGITAL oprește emiterea, revocă certificatele afectate, informează ADR, DNSC, titularii și părțile care se bazează, solicită actualizarea Listei de încredere și aplică, după caz, Planul de încetare. Certificatul CA este revocat de CERTDIGITAL ROOT CA G5, iar revocarea se publică imediat în CRL-ul autorității rădăcină.

La compromiterea sau suspiciunea de compromitere a cheii CERTDIGITAL ROOT CA G5, întreaga ierarhie G5 se consideră afectată: CERTDIGITAL revocă certificatul CERTDIGITAL QCA G5 și certificatele emise de aceasta, informează ADR, DNSC, titularii și părțile care se bazează, solicită retragerea certificatelor G5 din Lista de încredere și aplică, după caz, Planul de încetare pentru generația G5. Generația G4 nu este afectată, deoarece nu există certificare încrucișată.

5.7.4. Continuitatea activității după un dezastru

Pentru serviciile acoperite de prezenta DPC se aplică următoarele durate maxime de restabilire (RTO) și pierderi maxime de date (RPO): OCSP, CRL și depozitul de certificate — 4 ore / cel mult 5 minute; primirea și procesarea cererilor de revocare — 24 de ore / cel mult 5 minute; emiterea certificatelor — 72 de ore / cel mult 5 minute pentru baza de date CA. Centrul de date secundar se activează atunci când întreruperea estimată depășește RTO-ul serviciului afectat. Comutarea se testează cel puțin anual.

5.8. Încetarea activității CA sau RA

Încetarea unui serviciu de încredere se face conform Planului de încetare a serviciilor (00r), publicat pe site, și anexei acestuia pentru serviciul respectiv. ADR este informată cu cel puțin 3 luni înainte (art. 24 alin. (2) lit. (a) din Regulamentul eIDAS), iar în cazul unei încetări neprevăzute, în cel mult 24 de ore. Titularii și părțile care se bazează sunt informați în termenele prevăzute în plan. Informațiile privind starea certificatelor rămân disponibile și după încetare (art. 24 alin. (4) din Regulamentul eIDAS), prin succesor sau custode, inclusiv ultima CRL emisă

înaintea distrugerii cheii autorității de certificare. Ultima CRL se emite numai după ce toate certificatele din domeniul ei au expirat sau au fost revocate și are nextUpdate „99991231235959Z” (ETSI EN 319 411-1, CSS-6.3.9-06; ETSI EN 319 411-2, CSS-6.3.10-07 și CSS-6.3.10-09). Integritatea și disponibilitatea ultimei CRL se păstrează cel puțin pe durata de păstrare a înregistrărilor (CSS-6.3.10-08). Înainte de expirarea certificatului unei autorități, CERTDIGITAL calculează, pentru fiecare certificat emis de aceasta, un ultim răspuns OCSP cu nextUpdate „99991231235959Z” (CSS-6.3.10-11). Înregistrările se păstrează 10 ani prin custode. Cheile private ale autorităților se distrug pe bază de proces-verbal.

Retragerea unei autorități de certificare dintr-o generație (de exemplu G3) nu reprezintă încetarea serviciului, dacă serviciul continuă printr-o altă generație. Aceasta se tratează ca modificare (secțiunea 9.12).

6. Controale tehnice de securitate

6.1. Generarea și instalarea perechii de chei

6.1.1. Generarea perechii de chei

Cheile autorităților și ale certificatelor de serviciu. Perechile de chei CERTDIGITAL ROOT CA G5, CERTDIGITAL QCA G5 și ale certificatelor de serviciu G5 au fost generate într-o singură ceremonie a cheilor, pe 23.10.2026, direct în modulul criptografic Thales Luna în care se folosesc (secțiunea 6.2.1), sub control multipersoană (secțiunea 6.2.2). Ceremonia este consemnată în procesele-verbale nr. 68658–68661 (secțiunea 7.1.11), care consemnează și abaterile de la practica descrisă în prezenta secțiune (martorul independent, înregistrarea video, partițiile), cu măsurile de remediere. Remedierea se face într-o ceremonie desfășurată conform Procedurii privind generarea cheilor (PO_SI_72), cu martor independent și înregistrare video: cheile se relocă pe partițiile proprii, iar cheia CERTDIGITAL QEAA SERVICE G5 se generează din nou, direct în partiția SVG5, cu certificat nou emis de CERTDIGITAL QCA G5; cheia ei din 23.10.2026, nefolosită, se distruge, iar certificatul ei se revocă. Au fost emise, în ordine: certificatul autorității rădăcină; certificatul autorității subordonate, emis de autoritatea rădăcină; certificatele de serviciu, emise de autoritatea subordonată; apoi s-au făcut copiile de rezervă (secțiunea 6.2.4). Fiecare cheie se folosește pe partiția proprie: ROOTG5 (autoritatea rădăcină), CAG5 (autoritatea subordonată) și SVG5 (certificatele de serviciu); partiția autorității rădăcină se activează numai în ceremonii. Ceremoniile următoare (de exemplu, înlocuirea cheilor sau emiterea CRL-ului autorității rădăcină) se desfășoară sub control multipersoană, în prezența unui martor independent, cu înregistrare video și cu proces-verbal semnat de participanți.

Cheile titularilor. Perechea de chei a titularului se generează în dispozitivul criptografic al titularului (secțiunea 6.2.11): fie de CERTDIGITAL, la emitere, fie de titular, prin aplicația CertDigital CSR. Cheia privată nu părăsește dispozitivul.

Cheile din serviciul rQSCD. Perechea de chei se generează de CERTDIGITAL în dispozitivul calificat la distanță (secțiunea 6.2.11), la cererea titularului și după verificarea identității acestuia. Cheia privată nu părăsește dispozitivul decât sub forma copiilor de rezervă criptate de la secțiunea 6.2.4. Cheia de unică folosință se generează la cererea titularului, în sesiunea de semnare, după verificarea identității pentru certificatul respectiv (secțiunea 3.2.3) și după autentificarea titularului cu aplicația CertDigital ID, imediat înainte de cererea de certificare; ea nu se generează în avans și este legată de exact o sesiune de semnare (ETSI TS 119 431-1, GEN-6.2.1-07 și GEN-6.2.1-09). Titularul aprobă documentul sau lotul de documente de semnat, printr-o singură autorizare (SAD), după emiterea certificatului, astfel încât SAD se referă la cheia generată pentru sesiune.

6.1.2. Livrarea cheii private către titular

Nu se livrează chei private în fișiere. Dispozitivul cu cheia generată de CERTDIGITAL se predă titularului personal sau prin curier; datele de activare (PIN/PUK) se transmit în plic sigilat, separat de dispozitiv și prin alt curier decât cel care livrează dispozitivul.

Pentru serviciul rQSCD, cheia privată nu se livrează: ea rămâne în dispozitivul calificat la distanță, iar titularul primește mijlocul de autentificare cu care o activează (aplicația CertDigital ID).

6.1.3. Livrarea cheii publice către emitentul certificatului

Cheia publică a titularului se transmite către CA într-o cerere PKCS#10 semnată, prin canalul securizat dintre aplicațiile CertDigital și RA. Pentru cheile autorităților și ale certificatelor de serviciu G5, cheia publică se transmite emitentului în ceremonie, pe gazda modulului criptografic, într-o cerere PKCS#10 semnată cu cheia privată din modul (secțiunea 6.1.1).

6.1.4. Livrarea cheii publice a CA către părțile care se bazează

Certificatele CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5 sunt publicate la http://certs.certdigital.ro/ și în Lista de încredere a României. Amprentele SHA-256 ale certificatelor sunt publicate în depozit.

6.1.5. Dimensiunea cheilor

Cheie	Algoritm și dimensiune
CERTDIGITAL ROOT CA G5, CERTDIGITAL QCA G5	RSA 4096
Certificatele de serviciu QESVAL, QPS, QEARCH, QLEDGERS, QREM și QERDS SERVICE G5	RSA 4096
CERTDIGITAL OCSP G5 și CERTDIGITAL TSA G5	RSA 3072
CERTDIGITAL QEAA SERVICE G5	ECDSA pe curba NIST P-256
Certificatele titularilor emise până la 28.02.2027	RSA 2048
Certificatele titularilor emise de la 01.03.2027	ECDSA pe curba NIST P-256
Certificatele pentru chei gestionate în QSCD la distanță (serviciul rQSCD)	RSA de cel puțin 3072 de biți sau ECDSA pe curbele NIST P-256 / P-384 (secțiunea 7.1.2)

Certificatele și listele de revocare emise de CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5 sunt semnate cu sha512WithRSAEncryption. Cheia ECDSA P-256 a certificatului CERTDIGITAL QEAA SERVICE G5 este impusă de formatele atestatelor electronice ale atributelor (ISO/IEC 18013-5 și SD-JWT VC, algoritmul ES256). Algoritmii și lungimile de cheie se aleg după documentul „Agreed Cryptographic Mechanisms” v2 al ECCG (ENISA) și după ETSI TS 119 312 V2.1.1. Semnătura RSA PKCS#1 v1.5 (sha512WithRSAEncryption) este, în ambele documente, un mecanism „legacy” admis (în ETSI TS 119 312: L, cu termenul 31.12.2034) și se folosește pentru compatibilitatea cu aplicațiile de

validare; schema recomandată este RSASSA-PSS. Algoritmul de semnătură al autorităților G5 se reevaluează la fiecare revizuire a ETSI TS 119 312 și a documentului ECCG. Înainte ca semnătura RSA PKCS#1 v1.5 să nu mai fie admisă (în prezent, 31.12.2034), certificatele și CRL-urile noi se semnează cu RSASSA-PSS sau autoritățile G5 se înlocuiesc cu o generație nouă. Cheile RSA 2048 ale titularilor se utilizează numai în perioada de tranziție de mai sus, iar certificatele RSA 2048 emise până la 28.02.2027 rămân valabile până la expirare (cel mult 3 ani). De la 01.03.2027, cheile titularilor de pe token sunt ECDSA P-256, deoarece tokenul livrat (secțiunea 6.2.11) admite, în modul aprobat FIPS, numai RSA 2048 și ECDSA pe curbele P-256 / P-521. Termenul de 28.02.2027 se abate de la recomandarea ECCG (31.12.2025 pentru cheile RSA cu modulul sub 3000 de biți) și de la ETSI TS 119 312 V2.1.1, 8.4 (fără certificate noi cu astfel de chei după 31.12.2026, iar cele emise până atunci valabile cel mult până la 31.12.2028). Abaterea este justificată de tokenul livrat, care admite în modul aprobat FIPS numai RSA 2048 și ECDSA, și de durata trecerii titularilor la ECDSA P-256 (inițializarea tokenurilor, aplicația de generare a cererilor de certificat și testele de compatibilitate). ETSI EN 319 411-1 și ETSI EN 319 412-2 (GEN-4.2.2-1) trimit la ETSI TS 119 312 cu titlu de recomandare.

6.1.6. Generarea parametrilor cheii publice și verificarea calității

Cheile RSA ale autorităților și ale certificatelor de serviciu G5 se generează în modulul criptografic cu exponentul public e = 65537, conform recomandării ECCG ACM ($\log_2 e > 16$). Exponentul și lungimea fiecărei chei se verifică după generare, înainte de emiterea certificatului, iar rezultatul se consemnează în procesul-verbal al ceremoniei. Cheia ECDSA se generează pe curba NIST P-256.

Cheile titularilor se generează în dispozitivul criptografic, cu generatorul de numere aleatoare al acestuia.

6.1.7. Scopurile utilizării cheii (keyUsage X.509 v3)

Certificat	keyUsage
CERTDIGITAL ROOT CA G5, CERTDIGITAL QCA G5	keyCertSign, cRLSign (critic)
Semnătură și sigiliu (titulari, chei pe token), indiferent de algoritmul cheii	digitalSignature, nonRepudiation (critic)
Semnătură și sigiliu, chei gestionate în QSCD la distanță (serviciul rQSCD)	nonRepudiation (critic) (secțiunea 7.1.2)
CERTDIGITAL OCSP G5	digitalSignature (critic)
CERTDIGITAL QEARCH SERVICE G5 și CERTDIGITAL QLEDGERS SERVICE G5	nonRepudiation (critic)
Celelalte certificate de serviciu G5 (TSA, QESVAL, QPS, QREM, QERDS, QEAA)	digitalSignature, nonRepudiation (critic)

Certificatele de titular G5 nu conțin keyEncipherment și dataEncipherment; limitarea generației G4 privind certificatele cu chei RSA (DPC CERTDIGITAL G4, secțiunea 7.1.10) nu se aplică.

6.2. Protecția cheii private și controalele modulului criptografic

6.2.1. Standardele și controalele modulului criptografic

Cheile autorităților și ale certificatelor de serviciu G5 sunt păstrate în modulele **Thales Luna PCIe HSM 7 A790, firmware 7.8.5** (două module: unul principal și unul de rezervă / înaltă disponibilitate), certificate Common Criteria (NSCIB-CC-2400054-01), certificate ca dispozitiv calificat conform Regulamentului eIDAS (eIDAS-2400055-01), cu certificatele valabile 05.09.2025–05.09.2030, și certificate FIPS 140-3 (certificatul CMVP nr. 4684).

Cheile sunt separate pe partiții, fiecare cu propriile date de autentificare:

Partiție	Conținut	Utilizare
ROOTG5	cheia CERTDIGITAL ROOT CA G5	activată numai în ceremonii
CAG5	cheia CERTDIGITAL QCA G5	folosită de aplicația CA
SVG5	cheile certificatelor de serviciu G5	folosite de aplicațiile serviciilor

6.2.2. Controlul multipersoană (M din N) al cheii private

Activarea, copierea de rezervă și restaurarea cheilor autorităților necesită prezența simultană a cel puțin două persoane cu roluri de încredere (custozi HSM). Modulele Luna A790 folosesc autentificarea prin parolă; parolele partițiilor și secretul domeniului de clonare sunt împărțite în componente deținute de custozi diferiți, astfel încât nicio persoană nu poate activa sau copia singură o cheie a autorității. Persoanele care au introdus componentele se consemnează în procesul-verbal.

6.2.3. Păstrarea în custodie a cheii private

Cheile private ale autorității nu se încredințează terților. Cheile titularilor aflate pe dispozitivul acestora nu se păstrează de CERTDIGITAL; cheile din serviciul rQSCD se păstrează în dispozitivul calificat la distanță, în condițiile secțiunii 4.12.

6.2.4. Copia de rezervă a cheii private

Copia de rezervă a cheilor autorităților și ale certificatelor de serviciu G5 se realizează sub control multipersoană, cu proces-verbal: partițiile se copiază criptat pe un dispozitiv de backup Thales Luna Backup HSM și se restaurează în al doilea modul Luna A790 (secțiunea 6.2.1). Dispozitivul de backup se păstrează offline, într-un seif, în afara centrelor de date, sub custodia unei persoane desemnate. Cheile nu ies din modulele Thales decât criptate, în cadrul aceluiași domeniu de clonare. Nu se fac copii de rezervă ale cheilor titularilor aflate pe dispozitivul acestora. Pentru serviciul rQSCD, copiile de rezervă se realizează numai prin mecanismele interne ale dispozitivului certificat, criptat, cu același nivel de securitate ca originalul și în numărul minim

necesar continuității serviciului (art. 29a alin. (1) lit. (b) din Regulamentul eIDAS; PDP-rQSCD, secțiunea 6.8). Pentru cheile de unică folosință se aplică secțiunea 4.12.1.

6.2.5. Arhivarea cheii private

Cheile private ale autorității nu se arhivează după încetarea utilizării; ele se distrug conform secțiunii 6.2.10.

6.2.6. Transferul cheii private în sau din modulul criptografic

Cheile G5 se generează direct în modulul în care se folosesc și nu se transferă. Singurele copii sunt cele criptate de la secțiunea 6.2.4, pe dispozitivul de backup și în al doilea modul Luna A790. Dacă un modul se scoate din uz, cheile din el se distrug (zeroizare) sub control dual, cu proces-verbal.

6.2.7. Stocarea cheii private în modulul criptografic

Cheile private sunt generate și păstrate în HSM și nu există niciodată în clar în afara acestuia.

6.2.8. Metoda de activare a cheii private

Cheia CERTDIGITAL QCA G5 se activează în modul prin autentificarea custozilor, sub control dual (secțiunea 6.2.2). În funcționarea curentă, utilizarea cheii este permisă numai aplicației CA, prin canalul autentificat cu modulul. Cheile certificatelor de serviciu sunt utilizabile numai de aplicațiile serviciilor respective, prin canalul autentificat cu partiția SVG5.

Partiția autorității rădăcină (ROOTG5) se activează numai în ceremonii (emiterea sau revocarea certificatului autorității subordonate, emiterea CRL-ului autorității rădăcină) și se dezactivează la finalul fiecăreia. În afara ceremoniilor, cheia CERTDIGITAL ROOT CA G5 nu poate fi folosită.

Cheia titularului se activează prin introducerea PIN-ului dispozitivului, de către titular.

Cheia din serviciul rQSCD se activează numai de modulul de activare a semnăturii (SAM) al dispozitivului calificat la distanță, pe baza datelor de activare a semnăturii (SAD), generate după autentificarea titularului cu aplicația CertDigital ID și aprobarea explicită a datelor de semnat (nivelul SCAL2 din EN 419 241-1). Cheia de unică folosință se activează numai în sesiunea de semnare de care este legată, pe baza unei singure aprobări a titularului pentru documentul sau lotul de documente din sesiune.

6.2.9. Metoda de dezactivare a cheii private

Cheia CA se dezactivează la oprirea serviciului sau la închiderea sesiunii HSM. Cheia titularului se dezactivează la scoaterea dispozitivului sau la închiderea sesiunii. Cheia din serviciul

rQSCD rămâne inactivă în afara activărilor autorizate prin SAD. Cheia de unică folosință nu mai poate fi activată după încheierea sesiunii, deoarece se șterge (secțiunea 6.2.10).

6.2.10. Metoda de distrugere a cheii private

Cheile autorității se distrug prin zeroizarea lor în HSM și a copiilor de rezervă, sub control dual, cu proces-verbal. Cheia titularului se distruge prin ștergerea ei din dispozitiv sau prin distrugerea fizică a dispozitivului. Cheile din serviciul rQSCD și copiile lor de rezervă se distrug în dispozitivul calificat la revocarea sau expirarea certificatului, la cererea titularului și la încetarea serviciului, iar cheile de unică folosință, imediat după încheierea sesiunii de semnare, inclusiv când sesiunea expiră sau nu se finalizează (ETSI TS 119 431-1, DEL-6.3.2-05; CEN EN 419 241-1, SRG_KM.7.2; PDP-rQSCD, secțiunea 6.7). Ștergerea elimină cheia criptată, identificatorul ei și cheia publică din baza de date a dispozitivului și din replica ei, prin operația de ștergere a dispozitivului certificat, și se jurnalizează.

6.2.11. Evaluarea modulului criptografic

HSM-ul autorității: conform secțiunii 6.2.1.

Dispozitivul calificat la distanță (serviciul rQSCD): Ascertia ADSS Server SAM Appliance v7.0.2, dispozitiv calificat la distanță pentru semnătură și sigiliu, certificat de OCSI (OCSI/ACC/ASC/01/2022/RA, în vigoare din 23.05.2022) și înscris pe lista Comisiei Europene a dispozitivelor calificate, cu modulul criptografic Utimaco CryptoServer CP5 Se500 (NSCIB-CC-2300142-01, firmware 5.1.0.0). Detaliile sunt în PDP-rQSCD, secțiunea 4.2.

Dispozitivele titularilor: CERTDIGITAL livrează un singur model de token USB, token certificat (dispozitiv calificat de creare a semnăturilor și a sigiliilor):

Element	Valoare
Model	Century Longmai mToken CryptoID (variantele CryptoID-K9 și CryptoID-A3), firmware 3.12
Certificare	token certificat (QSCD); FIPS 140-3, nivelul general de securitate 3, certificatul CMVP nr. 4845 (21.10.2024)
Algoritmi în modul aprobat FIPS	RSA 2048; ECDSA pe curbele P-256 și P-521; SHA-2

Tokenul este livrat de producător în modul neaprobat. CERTDIGITAL îl inițializează în modul aprobat FIPS înainte de generarea cheilor și verifică indicatorul de stare (LED verde aprins continuu), conform politicii de securitate a modulului. Certificatele emise anterior pe alte modele de token rămân valabile până la expirare sau revocare.

6.3. Alte aspecte ale gestionării perechii de chei

6.3.1. Arhivarea cheii publice

Cheile publice se arhivează ca parte a certificatelor, conform secțiunii 5.5.

6.3.2. Perioadele de valabilitate ale certificatelor și de utilizare a cheilor

Certificat	Valabilitate
CERTDIGITAL ROOT CA G5	25 de ani de la ceremonia de generare a cheii
CERTDIGITAL QCA G5	15 ani de la ceremonia de generare a cheii
Certificatele de serviciu G5	CERTDIGITAL OCSP G5 și CERTDIGITAL TSA G5: 3 ani; certificatele celorlalte servicii: 5 ani; la înlocuire se generează o cheie nouă. Cheia CERTDIGITAL TSA G5 se utilizează cel mult 2 ani de la emiterea certificatului, deci mai puțin decât valabilitatea acestuia (ETSI EN 319 421, TIS-7.6.7-04)
Certificatele titularilor	cel mult 3 ani
Certificatele cheilor de unică folosință (serviciul rQSCD)	cel mult 60 de minute de la emitere, fără antedatare; certificate de scurtă durată, a căror valabilitate este mai mică decât termenul maxim de prelucrare a unei cereri de revocare (24 de ore, secțiunea 4.9.5; ETSI EN 319 411-1, clauza 3.1)

Cheia privată a titularului se utilizează numai pe durata valabilității certificatului. Cheia de unică folosință se utilizează numai în sesiunea de semnare de care este legată, în perioada de valabilitate a certificatului ei, și se șterge imediat după încheierea sesiunii (secțiunea 6.2.10); semnăturile și sigiliile create cu ea conțin o marcă temporală calificată aplicată în această perioadă (nivelul B-T sau superior), pe baza căreia se validează și după expirarea certificatului.

6.4. Datele de activare

6.4.1. Generarea și instalarea datelor de activare

Pentru dispozitivele cu chei generate de CERTDIGITAL, PIN-ul și PUK-ul inițiale se generează aleatoriu și se transmit titularului în plic sigilat, separat de dispozitiv și prin alt curier decât cel care livrează dispozitivul. Când titularul generează cheia prin aplicația CertDigital CSR, acesta stabilește singur PIN-ul.

Titularul are obligația să schimbe codul PIN înainte de prima utilizare a cheii private.

Datele de activare ale HSM (componentele parolelor deținute de custozi) sunt stabilite în ceremonie și sunt cunoscute numai deținătorilor lor.

6.4.2. Protecția datelor de activare

Titularul păstrează PIN-ul secret și separat de dispozitiv. Dispozitivul se blochează după un număr limitat de încercări greșite. Custozii HSM nu dezvăluie componentele parolelor; eventualele copii scrise se păstrează în plicuri sigilate, în seifuri individuale.

6.4.3. Alte aspecte ale datelor de activare

Nu se aplică.

6.5. Controale de securitate a sistemelor informatice

6.5.1. Cerințe tehnice specifice

Sistemele CA, RA și OCSP: rulează pe sisteme de operare securizate (hardening), cu actualizări de securitate aplicate controlat; impun autentificare cu cel puțin doi factori pentru accesul administrativ; separă rolurile; jurnalizează evenimentele (secțiunea 5.4); sunt protejate împotriva programelor malițioase. Măsurile respectă ETSI EN 319 401 și art. 21 din Directiva (UE) 2022/2555.

6.5.2. Evaluarea securității sistemelor

Sistemele sunt evaluate în cadrul evaluării de conformitate (capitolul 8) și prin testele de la secțiunea 5.4.8.

6.6. Controale tehnice privind ciclul de viață

6.6.1. Controlul dezvoltării sistemelor

Aplicațiile CertDigital (CA, RA, KYC, CertDigital CSR, client de certificare) sunt dezvoltate intern, cu separarea mediilor de dezvoltare, test și producție, revizuirea codului și testarea înainte de punerea în producție.

6.6.2. Controlul gestionării securității

Modificările de configurație și de programe în producție urmează procedura de gestionare a schimbărilor, cu aprobare, testare și jurnalizare.

6.6.3. Controalele de securitate ale ciclului de viață

Integritatea programelor se verifică la instalare; versiunile sunt ținute sub control.

6.7. Controale de securitate a rețelei

Rețeaua este segmentată pe zone de securitate; operațiile autorității rădăcină se efectuează numai în ceremonii (secțiunea 6.2.8). Între zone sunt permise numai fluxurile necesare serviciilor, prin firewall-uri cu filtrare și monitorizare; administrarea se face numai din rețeaua internă dedicată. Comunicațiile cu RA și cu clienții sunt criptate (TLS). Detaliile topologiei sunt descrise în documentația internă.

6.8. Marcarea temporală

Toate sistemele serviciilor sunt sincronizate cu sursa de timp UTC a CERTDIGITAL, descrisă în documentul „Sursa de timp” (00u): două servere de timp GNSS, câte unul în fiecare centru de date, și o sursă independentă de GNSS (NIST). Certificatele, CRL-urile, răspunsurile OCSP și jurnalele se emit în timp UTC.

7. Profilurile certificatelor, CRL și OCSP

7.1. Profilul certificatelor

7.1.1. Numărul versiunii

Toate certificatele sunt X.509 versiunea 3 (RFC 5280).

7.1.2. Extensiile certificatelor

Certificatele titularilor

Câmp / extensie	Semnătură (persoană fizică)	Sigiliu (persoană juridică)
serialNumber	unic, pozitiv, 16 octeți, cu componentă aleatoare	idem
signature	sha512WithRSAEncryption	idem
issuer	C=RO, O=CENTRUL DE CALCUL S.A., OU=CERTDIGITAL, organizationIdentifier=VATRO-2163993, CN=CERTDIGITAL QCA G5	idem
validity	cel mult 3 ani (certificatele cheilor de unică folosință din serviciul rQSCD: cel mult 60 de minute, tabelul de mai jos)	idem
subject	secțiunea 3.1.1	secțiunea 3.1.1
subjectPublicKeyInfo	RSA 2048 (până la 28.02.2027); ECDSA P-256 (de la 01.03.2027)	idem
authorityKeyIdentifier	numai keyIdentifier (fără numele și numărul de serie ale emitentului)	idem
subjectKeyIdentifier	SHA-1 al cheii publice (RFC 5280, metoda 1)	idem
keyUsage (critic)	digitalSignature, nonRepudiation, indiferent de algoritmul cheii	idem
extKeyUsage (necritic)	documentSigning Microsoft (1.3.6.1.4.1.311.10.3.12) și clientAuth (1.3.6.1.5.5.7.3.2), pentru autentificarea titularului (secțiunea 1.4.1); fără alte scopuri	idem
certificatePolicies	QCP-n-qscd (0.4.0.194112.1.2) + politica CERTDIGITAL (secțiunea 1.2), cu CPS https://www.certdigital.ro/repository	QCP-l-qscd (0.4.0.194112.1.3) + politica CERTDIGITAL, cu CPS
cRLDistributionPoints	http://crl.certdigital.ro/certdigital_qualified_g5.crl	idem
authorityInfoAccess	OCSP http://ocsp.g5.certdigital.ro; caIssuers http://certs.certdigital.ro/certdigital_qualified_g5.crt	idem
subjectAltName	rfc822Name (e-mail) și, după caz, UPN	idem
basicConstraints (critic)	CA:FALSE	idem

Câmp / extensie	Semnătură (persoană fizică)	Sigiliu (persoană juridică)
qcStatements	QcCompliance; QcSSCD; QcType = eSign (0.4.0.1862.1.6.1); QcPDS cu două locații: https://www.certdigital.ro/repository/pds/certdigital_pds_en.pdf (en) și https://www.certdigital.ro/repository/pds/certdigital_pds_ro.pdf (ro); de la 01.03.2027, declarația semantică 0.4.0.194121.1.1	QcCompliance; QcSSCD; QcType = eSeal (0.4.0.1862.1.6.2); QcPDS (en, ro); de la 01.03.2027, declarația semantică 0.4.0.194121.1.2
1.3.6.1.4.1.47898.30.1 (necritic)	legătura cu documentul de identificare verificat (paragraful de sub tabel)	—

Extensia 1.3.6.1.4.1.47898.30.1. Conține, ca DerIA5String, valoarea hexazecimală a unei amprente calculate asupra șirului `{CodȚară}-{TipDocument}-{SerieDocument}-{CNP}-{DataEmiterii}-{DataExpirării}` (datele în format aaaallzz). Pentru certificatele emise până la 28.02.2027, amprenta este SHA-256; pentru certificatele emise de la 01.03.2027, valoarea este HMAC-SHA-256 calculat cu o cheie secretă păstrată în HSM, astfel încât să nu poată fi verificată sau reconstituită de terți. Extensia permite CERTDIGITAL să lege certificatul de documentul de identificare verificat; ea nu se utilizează de părțile care se bazează. Prelucrarea este descrisă în Politica de protecție a datelor (00d).

Certificatele pentru chei gestionate în QSCD la distanță (serviciul rQSCD). Au profilul certificatelor titularilor de mai sus, cu următoarele diferențe:

Câmp / extensie	Valoare
validity	chei de lungă durată: cel mult 3 ani; chei de unică folosință: cel mult 60 de minute, cu notBefore egal cu momentul emiterii, fără antedatare (secțiunea 6.3.2)
subjectPublicKeyInfo	RSA ≥ 3072 sau ECDSA pe curbele NIST P-256 / P-384 (PDP-rQSCD, secțiunea 13.1.2)
keyUsage (critic)	nonRepudiation (ETSI EN 319 412-2, cl. 4.3.2)
extKeyUsage	nu se include
certificatePolicies	QCP-n-qscd sau QCP-l-qscd + 1.3.6.1.4.1.47898.5.2.2.{1,4,6}.{1,2} + 1.3.6.1.4.1.47898.11.1.1 (chei de lungă durată) sau 1.3.6.1.4.1.47898.5.2.2.{1,4}.{1,2} + 1.3.6.1.4.1.47898.11.1.2 (chei de unică folosință; codul de identificare 1 sau 4, secțiunea 3.2.3) + EUSPv2 (0.4.0.19431.1.1.4), cu CPS https://www.certdigital.ro/repository
qcStatements	QcCompliance; QcSSCD (cheia se află în dispozitivul calificat la distanță, secțiunea 6.2.11); QcType eSign sau eSeal; QcPDS (en și ro, ca la certificatele titularilor)
cRLDistributionPoints, authorityInfoAccess	ca la certificatele titularilor, inclusiv în certificatele de scurtă durată ale cheilor de unică folosință, care sunt revocabile (secțiunea 4.9.3)
extensia validity-assured (0.4.0.194121.2.1, ETSI EN 319 412-1) și extensia noRevAvail (IETF RFC 9608)	nu se includ (ETSI EN 319 411-1, GEN-6.6.1-04)

Certificatele serviciului rQSCD se emit numai după ce profilul configurat în CA a fost verificat față de tabelul de mai sus, pe câte un certificat de test pentru cheile de lungă durată și pentru cheile de unică folosință.

Certificatele de serviciu ale prestatorului

Certificat	Chei e	keyUsage (critic)	extKeyUsage	Politici
CERTDIGITAL OCSP G5	RSA 3072	digitalSignature	OCSPSigning (critic)	1.3.6.1.4.1.47898.5.2.2.1.2
CERTDIGITAL TSA G5	RSA 3072	digitalSignature, nonRepudiation	timeStamping (critic)	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2
CERTDIGITAL QESVAL SERVICE G5	RSA 4096	digitalSignature, nonRepudiation	—	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.9.1
CERTDIGITAL QPS SERVICE G5	RSA 4096	digitalSignature, nonRepudiation	—	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.10.1
CERTDIGITAL QEARCH SERVICE G5	RSA 4096	nonRepudiation	—	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.12.1
CERTDIGITAL QLEDGERS SERVICE G5	RSA 4096	nonRepudiation	—	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.13.1
CERTDIGITAL QREM SERVICE G5	RSA 4096	digitalSignature, nonRepudiation	emailProtection (necritic)	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.14.1
CERTDIGITAL QERDS SERVICE G5	RSA 4096	digitalSignature, nonRepudiation	—	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.14.1
CERTDIGITAL QEAA SERVICE G5	ECDSA P-256	digitalSignature, nonRepudiation	—	QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.15.1

Elementele comune ale certificatelor de serviciu G5:

– **subiect:** C=RO, O=CENTRUL DE CALCUL S.A., OU=CERTDIGITAL, organizationIdentifier=VATRO-2163993, CN conform tabelului;

– **număr de serie** aleator, pozitiv, de 20 de octeți (160 de biți); **valabilitate** 5 ani (CERTDIGITAL OCSP G5 și CERTDIGITAL TSA G5: 3 ani, iar cheia TSA se utilizează cel mult 2 ani); **semnătura** emitentului: sha512WithRSAEncryption; cheile RSA au e = 65537;

– **subjectKeyIdentifier:** SHA-1 al cheii publice; **authorityKeyIdentifier:** keyIdentifier; **basicConstraints:** CA:FALSE (critic);

– **cRLDistributionPoints:** http://crl.certdigital.ro/certdigital_qualified_g5.crl; **authorityInfoAccess:** OCSP http://ocsp.g5.certdigital.ro și caIssuers

http://certs.certdigital.ro/certdigital_qualified_g5.crt; certificatul OCSP are în authorityInfoAccess numai caIssuers;

– **qcStatements** (toate, cu excepția certificatului OCSP): QcCompliance, QcSSCD, QcType eSeal, QcPDS (en și ro, ca la certificatele titularilor) și declarația semantică pentru persoane juridice (0.4.0.194121.1.2);

– **certificatul OCSP** conține extensia id-pkix-ocsp-nocheck și nu conține qcStatements și subjectAltName; **certificatul QREM** conține în subjectAltName adresa de e-mail a serviciului, office@rem.certdigital.ro;

– calificativul CPS al fiecărei politici: https://www.certdigital.ro/repository.

Certificatele autorităților

Câmp / extensie	CERTDIGITAL ROOT CA G5	CERTDIGITAL QCA G5
subject	C=RO, O=CENTRUL DE CALCUL S.A., OU=CERTDIGITAL, organizationIdentifier=VATRO-2163993, CN=CERTDIGITAL ROOT CA G5	idem, CN=CERTDIGITAL QCA G5
issuer	identic cu subiectul (certificat autosemnat)	CERTDIGITAL ROOT CA G5 (DN complet)
serialNumber	aleator, pozitiv, 20 de octeți	idem
validity	25 de ani de la ceremonia de generare a cheii	15 ani de la ceremonia de generare a cheii
cheie și semnătură	RSA 4096, e = 65537; sha512WithRSAEncryption	idem
basicConstraints (critic)	CA:TRUE	CA:TRUE, pathLenConstraint = 0
keyUsage (critic)	keyCertSign, cRLSign	idem
subjectKeyIdentifier	SHA-1 al cheii publice	idem
authorityKeyIdentifier	— (certificat autosemnat)	keyIdentifier
certificatePolicies	—	anyPolicy (2.5.29.32.0), CPS https://www.certdigital.ro/repository
cRLDistributionPoints	—	http://crl.certdigital.ro/certdigital_root_g5.crl
authorityInfoAccess	—	caIssuers http://certs.certdigital.ro/certdigital_root_g5.crt (fără OCSP)

7.1.3. Identificatorii algoritmilor

– sha512WithRSAEncryption (1.2.840.113549.1.1.13) — semnarea tuturor certificatelor și CRL-urilor emise de CERTDIGITAL ROOT CA G5 și CERTDIGITAL QCA G5;

– rsaEncryption (1.2.840.113549.1.1.1) — cheile publice RSA;

– id-ecPublicKey (1.2.840.10045.2.1), cu curbele P-256 (1.2.840.10045.3.1.7) și P-384 (1.3.132.0.34) — cheile publice ECDSA: P-256 pentru certificatul CERTDIGITAL QEAA SERVICE G5 și pentru certificatele de pe token emise de la 01.03.2027; P-256 sau P-384 pentru cheile gestionate în QSCD la distanță (secțiunea 7.1.2).

7.1.4. Formele de nume

Conform secțiunii 3.1.

7.1.5. Constrângerile de nume

Nu se utilizează.

7.1.6. Identificatorul politicii de certificare

Conform secțiunii 1.2. Certificatele de serviciu G5 conțin și identificatorul politicii serviciului (tabelul din secțiunea 7.1.2): 1.3.6.1.4.1.47898.9.1 (validare), .10.1 (păstrare), .12.1 (arhivare), .13.1 (registre electronice), .14.1 (transmitere electronică înregistrată) și .15.1 (atestarea electronică a atributelor).

7.1.7. Utilizarea extensiei policyConstraints

Nu se utilizează.

7.1.8. Sintaxa și semantica calificativelor de politică

Calificativul CPS conține adresa depozitului: https://www.certdigital.ro/repository.

7.1.9. Prelucrarea extensiei certificatePolicies critice

Extensia certificatePolicies nu este marcată critică.

7.1.10. Diferențele față de profilurile generației G4

Profilurile G5 corectează limitările cunoscute ale profilurilor G4 (DPC CERTDIGITAL G4, secțiunea 7.1.10):

Element	Generația G4	Generația G5
Exponentul public al cheilor CA și de serviciu	mai mic de $2^{16}+1$	65537 (secțiunea 6.1.6)
Numerele de serie ale certificatelor de autoritate și de serviciu	secvențiale	aleatoare, 20 de octeți
keyUsage al certificatelor de titular cu chei RSA	include keyEncipherment și dataEncipherment	numai digitalSignature și nonRepudiation (secțiunea 6.1.7)
extKeyUsage	critic, cu scopuri suplimentare	necritic, cu excepția certificatelor TSA și OCSP
QcPDS	trimite la pagina depozitului	PDS-ul în engleză și în română, la adrese fixe
Certificatul OCSP	valabil 15 ani	valabil 3 ani, RSA 3072

Element	Generația G4	Generația G5
Algoritmul CRL-ului autorității subordonate	sha256WithRSAEncryption	sha512WithRSAEncryption, ca la certificate
Politicile CERTDIGITAL	arcul 1.3.6.1.4.1.47898.4	arcul 1.3.6.1.4.1.47898.5
Modulul criptografic al autorităților	Utimaco CryptoServer CP5	Thales Luna PCIe HSM 7 A790 (secțiunea 6.2.1)

Modificările aplicabile ambelor generații de la 01.03.2027 (atributul serialNumber cu prefix semantic, extensia 1.3.6.1.4.1.47898.30.1 calculată cu HMAC-SHA-256 și cheile ECDSA P-256 pentru titularii de pe token) sunt descrise în secțiunile 3.1.2, 6.1.5 și 7.1.2.

7.1.11. Certificatele emise la ceremonia din 23.10.2026

Certificatele generației G5 emise la ceremonia cheilor din 23.10.2026 se păstrează. Ele respectă profilurile din secțiunea 7.1.2, cu patru diferențe, consemnate și în procesele-verbale ale ceremoniei (nr. 68658–68661):

– **numerele de serie** sunt valori pozitive de 20 de octeți, fixate în șabloanele de generare, nu generate la emitere; aceleași valori au fost folosite în generările anterioare ale utilitarului, cu alte chei, iar certificatele acelor generări nu se publică și nu se folosesc;

– **notBefore** conține ora României înscrisă ca oră UTC, astfel că valabilitatea începe la 3 ore după semnare, în aceeași zi; certificatele nu sunt antedatate;

– **authorityKeyIdentifier** al certificatelor emise de CERTDIGITAL QCA G5 (CERTDIGITAL OCSP G5, CERTDIGITAL TSA G5 și cele 7 certificate de serviciu) conține, pe lângă keyIdentifier, numele și numărul de serie ale certificatului emitentului; certificatul CERTDIGITAL QCA G5 conține numai keyIdentifier, iar certificatul autosemnat CERTDIGITAL ROOT CA G5 nu conține extensia (RFC 5280, secțiunea 4.2.1.1);

– **certificatul CERTDIGITAL TSA G5** nu conține extensia privateKeyUsagePeriod; limita de cel mult 2 ani pentru utilizarea cheii TSA se aplică prin configurarea unității de marcare temporală (secțiunea 6.3.2).

Certificatele emise ulterior, inclusiv cele ale titularilor, și CRL-urile publicate respectă profilurile din secțiunile 7.1.2 și 7.2.

7.2. Profilul CRL

7.2.1. Numărul versiunii

CRL-urile sunt X.509 versiunea 2.

7.2.2. Extensiile CRL și ale intrărilor

Element	CRL CERTDIGITAL QCA G5	CRL CERTDIGITAL ROOT CA G5
issuer	CN=CERTDIGITAL QCA G5 (DN complet)	CN=CERTDIGITAL ROOT CA G5 (DN complet)
signature	sha512WithRSAEncryption	sha512WithRSAEncryption
thisUpdate / nextUpdate	emisă automat cel puțin la 8 ore și la fiecare revocare; nextUpdate = thisUpdate + 24 h	emisă cel puțin la 6 luni și la fiecare revocare de CA; nextUpdate = thisUpdate + 1 an
extensii	authorityKeyIdentifier (numai keyIdentifier), cRLNumber, expiredCertsOnCRL (secțiunea 4.10.1)	authorityKeyIdentifier (numai keyIdentifier), cRLNumber, expiredCertsOnCRL (secțiunea 4.10.1)
extensiile intrărilor	reasonCode	reasonCode
publicare	http://crl.certdigital.ro/certdigital_qualified_g5.crl	http://crl.certdigital.ro/certdigital_root_g5.crl

7.3. Profilul OCSP

7.3.1. Numărul versiunii

OCSP versiunea 1, conform IETF RFC 6960.

7.3.2. Extensiile OCSP

Răspunsurile sunt semnate cu certificatul de responder CERTDIGITAL OCSP G5 (RSA 3072, valabil 3 ani) și sunt de tip „basic”. Certificatul de responder conține extKeyUsage OCSPSigning și extensia id-pkix-ocsp-nocheck și nu conține metoda id-ad-ocsp în extensia authorityInfoAccess (ETSI EN 319 411-1, CSS-6.6.3-01A și CSS-6.6.3-01B). Serviciul acceptă extensia nonce (IETF RFC 6960) și răspunde „unknown” pentru certificatele care nu au fost emise de CERTDIGITAL QCA G5 (ETSI EN 319 411-1, OVR-6.6.3-02); cererile pentru astfel de certificate se monitorizează, ca posibil indiciu al unui atac (OVR-6.6.3-03). Răspunsurile conțin extensia archiveCutoff, cu data de început a valabilității certificatului CERTDIGITAL QCA G5 (secțiunea 4.10.1).

8. Evaluarea conformității și alte evaluări

8.1. Frecvența sau circumstanțele evaluării

Serviciile de încredere calificate sunt evaluate de un organism de evaluare a conformității (CAB) cel puțin o dată la 24 de luni, inclusiv în privința cerințelor de la art. 21 din Directiva (UE) 2022/2555 (art. 20 alin. (1) din Regulamentul eIDAS). Organismul de supraveghere poate dispune oricând un audit ad-hoc, pe cheltuiala CERTDIGITAL (art. 20 alin. (2)). CERTDIGITAL efectuează cel puțin anual un audit intern, realizat de personal independent de operarea serviciilor.

8.2. Identitatea și calificarea evaluatorului

Evaluarea este realizată de un CAB acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162 (EN ISO/IEC 17065 completat de ETSI EN 319 403-1 V2.3.1) de un organism național de acreditare.

8.3. Relația evaluatorului cu entitatea evaluată

CAB-ul este independent față de CERTDIGITAL și față de serviciile evaluate.

8.4. Subiectele acoperite de evaluare

Evaluarea acoperă serviciile de încredere calificate descrise în prezentul document, cerințele art. 24 din Regulamentul eIDAS și ale Regulamentului de punere în aplicare (UE) 2025/2530, precum și actele de punere în aplicare specifice serviciului (2025/1943, 2025/1566).

8.5. Acțiunile întreprinse ca urmare a neconformităților

Neconformitățile se remediază în termenul stabilit de organismul de supraveghere (cel mult 60 de zile). În lipsa remedierii, organismul de supraveghere poate retrage statutul calificat (art. 20 alin. (3)).

8.6. Comunicarea rezultatelor

ADR este informată cu cel puțin o lună înainte de evaluarea planificată și poate participa ca observator (art. 20 alin. (1a)). Raportul de evaluare se transmite ADR în cel mult 3 zile lucrătoare de la primire. Atestarea de conformitate se publică pe site.

9. Alte aspecte comerciale și juridice

9.1. Tarife

9.1.1. Tarifele pentru emiterea sau reînnoirea certificatelor

Tarifele serviciilor sunt cele din lista de tarife publicată pe site-ul https://www.certdigital.ro/ sau cele din oferta transmisă la cerere (art. 11 alin. (3) lit. b) din Legea nr. 214/2024).

9.1.2. Tarifele pentru accesul la certificate

Consultarea registrului public al certificatelor este gratuită.

9.1.3. Tarifele pentru accesul la informațiile de revocare sau de stare

Informațiile privind starea certificatelor (OCSP, CRL) sunt gratuite. Revocarea este gratuită.

9.1.4. Tarifele pentru alte servicii

Verificarea unei semnături la cererea unui terț (secțiunea 9.17) este gratuită. Pentru celelalte servicii se aplică lista de tarife.

9.1.5. Politica de rambursare

Conform contractului și, pentru consumatori, conform OUG nr. 34/2014.

9.2. Responsabilitatea financiară

9.2.1. Acoperirea prin asigurare

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, în condițiile art. 12 alin. (6) din Legea nr. 214/2024 și ale art. 5 alin. (2) lit. b) din procedura aprobată prin Ordinul MEDAT nr. 102/2026; în fiecare poliță, ADR, în calitate de organism de supraveghere, are calitatea de asigurat adițional. Polițele se reînnoiesc înainte de expirare; datele lor de identificare (asigurătorul, seria și numărul, perioada de valabilitate) sunt comunicate ADR și se pun la dispoziție la cerere.

9.2.2. Alte active

CERTDIGITAL dispune de resursele financiare necesare funcționării serviciului și aplicării Planului de încetare (00r, cap. 10).

9.2.3. Asigurarea sau garanția pentru entitățile finale

Nu se aplică.

9.3. Confidențialitatea informațiilor comerciale

9.3.1. Domeniul informațiilor confidențiale

Sunt confidențiale: datele din cereri care nu se înscriu în certificate, documentele de identificare, înregistrările video, jurnalele, documentația internă de securitate, cheile private și datele de activare.

9.3.2. Informațiile care nu sunt confidențiale

Certificatele (cu limitările de la secțiunea 2.2), CRL-urile, răspunsurile OCSP și documentele publicate în depozit.

9.3.3. Responsabilitatea pentru protejarea informațiilor confidențiale

Personalul CERTDIGITAL și terții care acționează în numele acestuia sunt obligați la păstrarea secretului profesional (art. 11 alin. (5) din Legea nr. 214/2024). Informațiile confidențiale se comunică numai în condițiile legii.

9.4. Protecția datelor cu caracter personal

9.4.1. Politica de confidențialitate

CERTDIGITAL prelucrează datele cu caracter personal ale titularilor, ale reprezentanților și ale solicitanților în calitate de operator, conform Regulamentului (UE) 2016/679 (GDPR), Legii nr. 190/2018 și Politicii de protecție a datelor cu caracter personal (00d, versiunea în vigoare, publicată la https://www.certdigital.ro/protectia-datelor/).

9.4.2. Informațiile tratate ca private

Datele de identificare, copiile actelor de identitate, înregistrările video și datele biometrice obținute la CERTDIGITAL KYC, codul numeric personal și datele de contact care nu se înscriu în certificat.

9.4.3. Informațiile care nu sunt considerate private

Datele înscrise în certificat, în măsura în care certificatul este prezentat de titular părților care se bazează sau este publicat cu acordul titularului.

9.4.4. Responsabilitatea pentru protejarea datelor

Temeiurile prelucrării sunt executarea contractului (art. 6 alin. (1) lit. b) GDPR) și îndeplinirea obligațiilor legale ale prestatorului de servicii de încredere calificat (art. 6 alin. (1) lit. c) GDPR; art. 24 din Regulamentul eIDAS; art. 16 din Legea nr. 214/2024). Compararea biometrică din CERTDIGITAL KYC se face pe baza consimțământului explicit (art. 9 alin. (2) lit. a) GDPR). Datele se păstrează conform secțiunii 5.5. Codul numeric personal se prelucrează

numai pentru verificarea identității și emiterea certificatelor, cu garanțiile prevăzute la art. 4 din Legea nr. 190/2018.

9.4.5. Notificarea și consimțământul pentru utilizarea datelor

Titularul este informat prin nota de informare din termenii și condiții și din formularele de cerere. Comunicările comerciale și descărcarea certificatului complet din registrul public se fac numai cu consimțământul separat al titularului, exprimat prin opțiuni nebifate implicit.

9.4.6. Dezvăluirea în cadrul procedurilor judiciare sau administrative

Datele se comunică autorităților și instanțelor numai în temeiul legii.

9.4.7. Alte situații de dezvăluire

Persoanele vizate au drepturile prevăzute la art. 15–22 GDPR și dreptul de a depune plângere la ANSPDCP. Responsabilul cu protecția datelor poate fi contactat la dpo@centruldecalcul.ro.

9.5. Drepturile de proprietate intelectuală

CERTDIGITAL deține drepturile asupra prezentei DPC, a certificatelor autorităților și a aplicațiilor proprii. Prezenta DPC poate fi reprodusă integral, fără modificări, cu indicarea sursei.

9.6. Declarații și garanții

9.6.1. Declarațiile și garanțiile CA

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 garantează că: datele din certificat sunt exacte la data emiterii; titularul identificat în certificat deținea, la emitere, cheia privată corespunzătoare cheii publice; cheile se corespund; informațiile de stare sunt disponibile conform secțiunii 4.10.

9.6.2. Declarațiile și garanțiile RA

Operatorii de înregistrare aplică procedurile de la capitolele 3 și 4.

9.6.3. Declarațiile și garanțiile titularilor

Titularul garantează că datele furnizate sunt exacte și complete și își respectă obligațiile de la secțiunea 4.5.1 (art. 26 din Legea nr. 214/2024).

9.6.4. Declarațiile și garanțiile părților care se bazează

Partea care se bazează își respectă obligațiile de la secțiunea 4.5.2.

9.6.5. Declarațiile și garanțiile altor participanți

Nu se aplică.

9.7. Exonerarea de garanții

CERTDIGITAL nu răspunde pentru prejudiciile rezultate din:

a) utilizarea certificatului sau a serviciului peste limitările notificate în prealabil și recognoscibile de terți (scopurile din extensiile keyUsage și extKeyUsage, politica indicată în certificat, perioada de valabilitate) (art. 13 alin. (2) din Regulamentul eIDAS; art. 15 alin. (5) din Legea nr. 214/2024);

b) nerespectarea de către titular a obligațiilor sale, inclusiv protejarea dispozitivului și a datelor de activare și solicitarea revocării în 24 de ore (art. 26 din Legea nr. 214/2024);

c) neverificarea de către partea care se bazează a stării certificatului (OCSP/CRL) și a statutului din Lista de încredere;

d) forța majoră.

9.8. Limitarea răspunderii

Nicio prevedere din prezentul document sau din contract nu exclude și nu limitează răspunderea CERTDIGITAL pentru prejudiciile cauzate cu intenție sau din culpă gravă (art. 1355 Cod civil). În raporturile cu consumatorii se aplică Legea nr. 193/2000. Clauzele privind răspunderea se acceptă în mod expres la încheierea contractului (art. 1203 Cod civil).

9.9. Despăgubiri

Răspunderea CERTDIGITAL este acoperită de asigurarea de la secțiunea 9.2. Titularul răspunde față de CERTDIGITAL pentru prejudiciile cauzate prin furnizarea de date false sau prin încălcarea obligațiilor sale.

9.10. Durata și încetarea

9.10.1. Durata

Prezenta DPC se aplică de la publicarea în depozit până la înlocuirea ei cu o versiune nouă.

9.10.2. Încetarea

La publicarea unei versiuni noi, versiunea anterioară încetează să se aplice certificatelor emise ulterior.

9.10.3. Efectul încetării și dispozițiile care rămân aplicabile

Pentru certificatele emise sub o versiune anterioară, prevederile privind răspunderea, păstrarea înregistrărilor și confidențialitatea rămân aplicabile până la expirarea perioadelor respective.

9.11. Notificările individuale și comunicarea cu participanții

Comunicările se fac prin e-mail, prin portalul client sau în scris, la datele de contact de la secțiunea 1.5.2 și la cele declarate de titular.

9.12. Modificări

9.12.1. Procedura de modificare

Orice modificare a prezentului document primește o versiune nouă, aprobată de Directorul General și publicată în depozitul de documente; versiunile anterioare rămân disponibile. Corecturile de redactare care nu modifică drepturile sau obligațiile părților se publică cu versiune nouă, fără termen de preaviz.

9.12.2. Mecanismul și termenul de notificare

Modificările care afectează prestarea serviciilor calificate se comunică ADR cu cel puțin o lună înainte de aplicare (cu cel puțin trei luni în cazul încetării unui serviciu). Titularii și părțile care se bazează sunt informați prin publicare pe site cu cel puțin 30 de zile înainte de intrarea în vigoare, timp în care titularii pot formula obiecții sau pot solicita revocarea certificatului, fără costuri.

9.12.3. Circumstanțele în care trebuie schimbat identificatorul de politică

Identificatorul de politică se schimbă dacă modificarea afectează nivelul de asigurare sau semnificația certificatelor emise.

9.13. Soluționarea litigiilor

Litigiile se soluționează pe cale amiabilă, pe baza unei reclamații transmise la office@certdigital.ro, la care 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 OG nr. 38/2015 (ANPC – https://anpc.ro/sal).

9.14. Legea aplicabilă

Prezentul document și raporturile juridice decurgând din furnizarea serviciilor sunt guvernate de dreptul român, sub rezerva dispozițiilor direct aplicabile ale dreptului Uniunii Europene.

9.15. Conformitatea cu legislația aplicabilă

Serviciile de încredere calificate ale CENTRUL DE CALCUL S.A. (CERTDIGITAL) sunt furnizate în conformitate cu:

a) Legislația Uniunii Europene

– Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 („Regulamentul eIDAS”);

– Regulamentul de punere în aplicare (UE) 2025/2530 privind cerințele pentru prestatorii de servicii de încredere calificați;

– Regulamentul de punere în aplicare (UE) 2025/1943 (standardele pentru certificatele calificate de semnătură și de sigiliu electronic) și Regulamentul de punere în aplicare (UE) 2025/1566 (verificarea identității, aplicabil de la 19.08.2027);

– Decizia de punere în aplicare (UE) 2016/650 (standardele pentru evaluarea securității dispozitivelor calificate de creare a semnăturilor și sigiliilor), cu trimitere la lista dispozitivelor certificate publicată de Comisia Europeană;

– Regulamentul de punere în aplicare (UE) 2026/248 (formatele de referință ale semnăturilor și sigiliilor avansate);

– Directiva (UE) 2022/2555 (NIS2) și Regulamentul de punere în aplicare (UE) 2024/2690;

– Regulamentul (UE) 2016/679 (GDPR).

b) Legislația națională

– Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, cu modificările și completările ulterioare;

– Ordinul ministrului economiei, digitalizării, antreprenoriatului și turismului nr. 102/2026 și deciziile Autorității pentru Digitalizarea României (ADR), în calitate de organism de supraveghere;

– Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, aprobată cu modificări prin Legea nr. 124/2025, cu modificările ulterioare;

– Legea nr. 190/2018 privind măsurile de punere în aplicare a GDPR și Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;

– Codul civil și, în raporturile cu consumatorii, Legea nr. 193/2000, Ordonanța de urgență a Guvernului nr. 34/2014 și Ordonanța Guvernului nr. 38/2015.

c) Standarde. Standardele aplicate sunt cele citate în actele de punere în aplicare de mai sus, în versiunile indicate acolo, conform listei de standarde publicate (documentul 00n). Versiunile mai noi sunt avute în vedere doar cu titlu informativ.

d) Ordinea de prevalență. În caz de neconcordanță se aplică, în ordine: Regulamentul eIDAS, actele de punere în aplicare, legislația națională, prezentul document. Dacă legislația națională impune o cerință suplimentară compatibilă cu Regulamentul eIDAS, se respectă ambele.

e) Organismul de supraveghere. Autoritatea pentru Digitalizarea României, București, www.adr.gov.ro.

9.16. Dispoziții diverse

9.16.1. Întregul acord

Raporturile cu titularul sunt guvernate de contract, de termenii și condițiile serviciului și de prezenta DPC.

9.16.2. Cesiunea

Titularul nu poate cesiona drepturile din contract fără acordul CERTDIGITAL.

9.16.3. Separabilitatea

Nulitatea unei prevederi nu afectează celelalte prevederi.

9.16.4. Executarea

Nu se aplică.

9.16.5. Forța majoră

Forța majoră se apreciază conform art. 1351 Cod civil.

9.17. Alte prevederi

Verificarea unei semnături la cererea unui terț. La cererea scrisă a oricărei persoane, transmisă la office@certdigital.ro sau la sediul CERTDIGITAL, însoțită de documentul semnat, CERTDIGITAL verifică dacă semnătura sau sigiliul a fost creat cu un certificat emis de CERTDIGITAL, starea certificatului la momentul semnării și integritatea semnăturii. Rezultatul se comunică în scris, sub forma unui raport semnat sau sigilat electronic, în cel mult 30 de zile de

la primirea cererii (art. 11 alin. (2) din Legea nr. 214/2024). Verificarea este gratuită și nu constituie un serviciu calificat de validare.

Accesibilitatea. CERTDIGITAL urmărește ca site-ul și documentele publicate în format PDF să respecte cerințele WCAG 2.1, nivel AA (EN 301 549), conform art. 15 din Regulamentul eIDAS și Legii nr. 232/2022. Persoanele cu dizabilități pot solicita asistență prin telefon (+40 253 214 767), prin e-mail (office@certdigital.ro) sau la sediu, inclusiv pentru verificarea identității prin prezență fizică.

Limba. Prezenta DPC este redactată în limba română. În caz de neconcordanță cu o traducere, prevalează versiunea în limba română.