

Politica și declarația de practici a serviciului calificat de registre electronice

CertDigital Ledgers

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, document unic: politica (Partea I) și declarația de practici (Partea a II-a) a serviciului calificat de registre electronice; Reg. (UE) 2025/2531; temeiul publicării tarifelor: art. 11 alin. (1) din Legea nr. 214/2024	22/10/2026
1.1	Ofițer de Securitate IT	Statutul calificat descris exact: pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României, iar până la înscriere serviciul nu se prestează ca serviciu 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	27/10/2026
1.2	Ofițer de Securitate IT	Tabelul de identificare arată versiunea și data în vigoare (în versiunea 1.1 rămăseseră cele ale versiunii 1.0)	27/10/2026
1.3	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

Cuprins

PARTEA I – Politica serviciului 8
1. Introducere 8
1.1. Prezentare generală 8
1.2. Identificarea documentului și a politicii 8
1.3. Participanții 9
1.4. Utilizarea serviciului 9
1.5. Administrarea documentului 9
2. Referințe normative 11
2.1. Acte normative și standarde 11
3. Definiții și acronime 12
3.1. Definiții 12
3.2. Acronime 12
4. Concepte generale 14
4.1. Serviciul și componentele sale 14
4.2. Arhitectura registrului 14
4.3. Profilul registrului centralizat (47898.13.1.1) 14
4.4. Datele cu caracter personal în registru 14
4.5. Identitatea serviciului și sigiliul serviciului 15
5. Politica serviciului 16
5.1. Identificare și conformitate 16
5.2. Comunitatea utilizatorilor și aplicabilitatea 16
5.3. Modificarea politicii 16
6. Cerințele privind practicile 17
6.1. Publicare și depozit 17
6.2. Termeni și condiții 17
6.3. Originea înregistrărilor 17
6.4. Ordonarea cronologică secvențială unică 17
6.5. Integritatea și detectarea modificărilor 18
6.6. Rapoartele de registru 18
6.7. Verificarea de către părțile care se bazează 18

6.8. Păstrarea registrului 18
6.9. Timpul de încredere și jurnalele 19
6.10. Personalul 19
6.11. Controale privind facilitățile, managementul și operarea 19
6.12. Controale criptografice 19
6.13. Protecția cheii serviciului și securitatea rețelei 19
6.14. Notificări către ADR și încetarea serviciului 20
6.15. Evaluarea conformității 20
7. Obligații și răspundere 21
7.1. Obligațiile CERTDIGITAL 21
7.2. Obligațiile abonatului și ale utilizatorilor 21
7.3. Obligațiile părților care se bazează 21
7.4. Răspunderea 21
7.5. Asigurarea 22
8. Alte aspecte comerciale și juridice 23
8.1. Tarife 23
8.2. Protecția datelor cu caracter personal 23
8.3. Modificări 23
8.4. Soluționarea litigiilor 23
8.5. Legea aplicabilă și cadrul legal 23
8.6. Alte prevederi 24
9. Corespondența cu cerințele Regulamentului (UE) 2025/2531 25
9.1. Tabel de corespondență 25
PARTEA A II-A – Declarația de practici 26
10. Publicare și depozit 26
10.1. Documentele și informațiile publicate 26
10.2. Informarea abonaților și a părților care se bazează 26
10.3. Revizuirea și modificarea documentului 26
11. Platforma registrului 28
11.1. Capacitățile funcționale 28
11.2. Arhitectura tehnică 28
11.3. Finalitatea înregistrărilor 29
12. Accesul la serviciu 30

12.1. Contractul și contul abonatului 30
12.2. Utilizatorii autorizați 30
12.3. Autentificarea 30
12.4. Interfața de programare 31
13. Înregistrarea datelor 32
13.1. Datele acceptate 32
13.2. Structura înregistrării 32
13.3. Verificarea originii 33
13.4. Ordonarea cronologică secvențială unică 33
13.5. Legătura criptografică 34
13.6. Mărcile temporale calificate 34
13.7. Sigilarea cu sigiliul calificat al serviciului 34
13.8. Punctele de control și ancorarea lor 35
13.9. Confirmarea înregistrării 35
13.10. Respingerea înregistrărilor 36
14. Verificarea de către părțile care se bazează 37
14.1. Dovezile puse la dispoziție 37
14.2. Verificarea prin interfața publică 37
14.3. Verificarea independentă 37
14.4. Verificarea ordinii și a integrității 38
14.5. Rapoartele de registru 38
15. Corecturi și imuabilitate 39
15.1. Imuabilitatea registrului 39
15.2. Corecturile 39
15.3. Neconcordanțele și erorile de operare 39
15.4. Datele cu caracter personal 39
16. Păstrarea, exportul și predarea registrului 41
16.1. Durata păstrării 41
16.2. Verificabilitatea pe termen lung și reînnoirea dovezilor 41
16.3. Schimbarea cheii serviciului 41
16.4. Exportul pentru abonat 41
16.5. Predarea registrului la încetarea serviciului 42
17. Controlul accesului și jurnalizarea 43

17.1. Rolurile și controlul accesului 43
17.2. Separarea datelor abonaților 43
17.3. Jurnalizarea 43
17.4. Verificarea continuă a consistenței 44
18. Controale operaționale 45
18.1. Evaluarea riscurilor 45
18.2. Cheile și modulele criptografice 45
18.3. Algoritmii și agilitatea criptografică 45
18.4. Personalul 46
18.5. Securitatea fizică 46
18.6. Securitatea rețelei 46
18.7. Monitorizarea 47
18.8. Continuitatea activității 47
18.9. Lanțul de aprovizionare 47
18.10. Gestionarea incidentelor 48
18.11. Compromiterea cheii serviciului 48
18.12. Încetarea serviciului 48
18.13. Evaluarea conformității și notificarea modificărilor 48
19. Aspecte juridice și comerciale 50
Anexa A – Corespondența practicilor cu Regulamentul de punere în aplicare (UE) 2025/2531 și cu Partea I 51

PARTEA I – Politica serviciului

1. Introducere

1.1. Prezentare generală

Prezentul document stabilește cerințele pe care CENTRUL DE CALCUL S.A. (marca CertDigital, denumită în continuare „CERTDIGITAL”), prestator de servicii de încredere calificat, le aplică la prestarea **serviciului calificat de înregistrare a datelor electronice în registre electronice calificate** (art. 3 pct. 52 și 53, art. 45k și 45l din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183) și descrie practicile prin care CERTDIGITAL le îndeplinește.

Serviciul permite abonaților să înregistreze date electronice într-un registru electronic administrat de CERTDIGITAL, care stabilește originea fiecărei înregistrări, asigură ordonarea lor cronologică secvențială unică și face ca orice modificare ulterioară să poată fi detectată imediat. Înregistrările din registrul electronic calificat beneficiază de prezumția ordonării lor cronologice secvențiale unice și exacte și de prezumția de integritate (art. 45k alin. (2)).

Politica (Partea I) stabilește **ce** garantează CERTDIGITAL. **Cum** sunt îndeplinite cerințele este descris în Partea a II-a (declarația de practici), cu conținutul minim cerut de Regulamentul de punere în aplicare (UE) 2025/2531 (REQ-6.1-12). Pentru mărcile temporale calificate folosite de serviciu se aplică Politica și declarația de practici a serviciului calificat de marcare temporală CertDigital (PDP-QTST), iar pentru cerințele comune tuturor serviciilor, Politicile generale CertDigital (PG).

1.2. Identificarea documentului și a politicii

Element	Valoare
Titlu	Politica și declarația de practici a serviciului calificat de înregistrare a datelor electronice în registre electronice calificate CertDigital (PDP-Ledgers)
Titlu în limba engleză	CertDigital Qualified Electronic Ledger Service Policy and Practice Statement
Versiune	1.3
Data	27.10.2026
Identificatorul documentului și al politicii (OID)	1.3.6.1.4.1.47898.13.1
Profilul registrului centralizat (OID)	1.3.6.1.4.1.47898.13.1.1: înregistrări de amprente criptografice, cu originea stabilită prin semnătura sau sigiliul utilizatorului, ordonate prin lanț de amprente și mărci temporale calificate și sigilate de CERTDIGITAL
Declarația de practici	declarația de practici este inclusă în prezentul document (Partea a II-a); identificatorul 1.3.6.1.4.1.47898.13.2 nu se mai folosește
Specificații de referință	ETSI EN 319 401 V3.1.1, cu adaptările din anexa la Regulamentul de punere în aplicare (UE) 2025/2531

Element	Valoare
Tipul de serviciu (ETSI TS 119 612)	`http://uri.etsi.org/TrstSvc/Svctype/Ledgers/Q`
Identitatea serviciului în Lista de încredere (după înscriere)	certificatul calificat de sigiliu al serviciului (secțiunea 4.5)
Generație	serviciul se prestează în generația G5 a infrastructurii CERTDIGITAL
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-ledgers_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Identificatorii sunt înscriși în CERTDIGITAL_OID_MAP. Certificatul de sigiliu al serviciului conține identificatorul politicii (1.3.6.1.4.1.47898.13.1), care identifică și prezentul document; identificatorul profilului se înscrie în înregistrări și în rapoartele de registru.

1.3. Participanții

– **prestatorul registrului**: CERTDIGITAL, care creează și administrează registrul și răspunde în ansamblu de serviciu, inclusiv atunci când folosește propriul serviciu calificat de marcare temporală;

– **abonatul**: persoana fizică sau juridică ce încheie contractul cu CERTDIGITAL pentru înregistrarea datelor în registru;

– **utilizatorii**: persoanele fizice sau juridice care, în numele abonatului, creează înregistrările și le semnează sau le sigilează cu propriul certificat calificat;

– **părțile care se bazează**: persoanele care verifică o înregistrare sau un raport de registru și se bazează pe acestea.

CERTDIGITAL nu deleagă către terți administrarea registrului, sigilarea sau gestionarea cheilor serviciului.

1.4. Utilizarea serviciului

Serviciul se utilizează pentru a dovedi existența, originea, ordinea și integritatea unor date la un anumit moment: de exemplu, amprentele documentelor, ale evenimentelor sau ale tranzacțiilor din procesele abonatului, jurnale de audit sau stări succesive ale unui registru de evidență. În registru se înscriu **numai amprente criptografice și metadatele minime necesare**, nu documentele în sine.

În registru **nu se înscriu date cu caracter personal în clar** (secțiunea 4.4). Datele la care se referă amprentele rămân la abonat.

1.5. Administrarea documentului

CENTRUL DE CALCUL S.A. (marca CertDigital), Str. Tudor Vladimirescu nr. 17, Târgu Jiu, județul Gorj, cod poștal 210132, România; J1991000103187; EUID ROONRC.J1991000103187; CUI RO2163993; tel. +40 253 214 767; office@certdigital.ro; https://www.certdigital.ro/.

Documentul este verificat de ofițerul de securitate IT și aprobat de Directorul General. Prezentul document este redactat în limba română; în caz de neconcordanță cu o traducere, prevalează versiunea în limba română.

2. Referințe normative

2.1. Acte normative și standarde

– Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183, art. 3 pct. 52 și 53, art. 13, 15, 20, 21, 24, 45k și 45l;

– Regulamentul de punere în aplicare (UE) 2025/2531 (standardele de referință și specificațiile pentru registrele electronice calificate);

– Regulamentul de punere în aplicare (UE) 2025/2530 (cerințe pentru prestatorii calificați: notificări, gestionarea riscurilor, planul de încetare);

– Regulamentul de punere în aplicare (UE) 2025/1929 (marcarea temporală calificată); Regulamentul de punere în aplicare (UE) 2025/1945 (validarea semnăturilor și sigiliilor electronice); Regulamentul de punere în aplicare (UE) 2025/2162 (acreditarea organismelor de evaluare a conformității);

– ETSI EN 319 401 V3.1.1 (cerințe generale pentru prestatorii de servicii de încredere);

– ETSI EN 319 122-1 V1.3.1 (CAdES), ETSI EN 319 132-1 V1.3.1 (XAdES), ETSI TS 119 182-1 V1.2.1 (JAdES) și IETF RFC 7515 (JWS);

– ETSI EN 319 102-1 (procedurile de validare a semnăturilor și sigiliilor AdES); ETSI EN 319 422 și IETF RFC 3161 (profilul și protocolul mărcilor temporale);

– EN ISO/IEC 17065 și ETSI EN 319 403-1 (evaluarea conformității prestatorilor de servicii de încredere);

– documentul „Agreed Cryptographic Mechanisms” al ECCG, publicat de ENISA; FIPS PUB 140-3; ISO/IEC 15408:2022; EN 419 221-5 (profilul de protecție al modulelor criptografice ale prestatorilor); Regulamentele de punere în aplicare (UE) 2024/482 și 2024/3144 (schema EUCC);

– ISO 23257:2022 și ISO/TS 23635:2022 — **nu se aplică**, deoarece registrul CERTDIGITAL nu folosește tehnologia registrelor distribuite (secțiunea 4.2);

– Regulamentul (UE) 2016/679, Legea nr. 190/2018 și Ghidul EDPB 02/2025 privind prelucrarea datelor cu caracter personal prin tehnologii blockchain (versiunea finală din 07.07.2026);

– Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026.

Lista completă a actelor normative și a standardelor aplicate este în documentul 00n.

3. Definiții și acronime

3.1. Definiții

– **registru electronic** — o secvență de înregistrări electronice de date, care asigură integritatea înregistrărilor respective și acuratețea ordinii cronologice a acestora (art. 3 pct. 52 din Regulamentul eIDAS);

– **registru electronic calificat** — registrul electronic pus la dispoziție de un prestator de servicii de încredere calificat, care îndeplinește cerințele de la art. 45l (art. 3 pct. 53);

– **înregistrare** — unitatea de date înscrisă în registru, cu identificatorul ei, poziția în secvență, amprenta datelor, metadatele, semnătura sau sigiliul utilizatorului și marca temporală;

– **legătură criptografică** — trimiterea la date stabilită prin tehnici criptografice adecvate, care asigură integritatea, autenticitatea sau trasabilitatea datelor și succesiunea corectă a înregistrărilor (RE 2025/2531, anexa, pct. 1 lit. (l));

– **raport de registru** — prezentarea structurată a unor informații verificabile extrase din înregistrările registrului (RE 2025/2531, anexa, pct. 1 lit. (m));

– **finalitate** — starea unei înregistrări care a devenit ireversibilă și nu mai poate fi modificată sau eliminată (RE 2025/2531, anexa, pct. 1 lit. (a));

– **punct de control** — starea registrului la un moment dat (amprenta capului lanțului sau rădăcina arborelui de amprente), sigilată de CERTDIGITAL și marcată temporal calificat;

– **confirmarea înregistrării** — înregistrarea sigilată de serviciu, transmisă utilizatorului după înscriere, cu identificatorul și poziția ei, amprenta ei și amprenta înregistrării anterioare (secțiunea 13.9);

– **dovadă de includere** — datele care permit recalcularea legăturii criptografice dintre o înregistrare și un punct de control (secțiunea 14.1);

– **amprentă cu componentă secretă** — amprenta calculată asupra datelor împreună cu o cheie sau cu o valoare aleatoare păstrată de abonat, astfel încât datele să nu poată fi deduse sau corelate pornind de la amprentă (secțiunea 4.4).

3.2. Acronime

Acronim	Semnificație
AdES	semnătură sau sigiliu electronic avansat (CAdES, XAdES, JAdES)
ADR	Autoritatea pentru Digitalizarea României, organismul de supraveghere
ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
API	interfață de programare a aplicațiilor
DLT	tehnologia registrelor distribuite
DNSC	Directoratul Național de Securitate Cibernetică
ECCG ACM	documentul „Agreed Cryptographic Mechanisms” al Grupului european de certificare a securității cibernetice

Acronim	**Semnificație**
GDPR	Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor)
HSM	modul criptografic hardware
JWS	JSON Web Signature (RFC 7515)
Ledgers/Q	serviciul calificat de înregistrare a datelor electronice în registre electronice calificate
QTST	marcă temporală electronică calificată
RTO / RPO	durata maximă de restabilire a serviciului / pierderea maximă de date admisă la restabilire
TLS	protocolul Transport Layer Security
UTC	timpul universal coordonat

4. Concepte generale

4.1. Serviciul și componentele sale

Serviciul cuprinde:

– **primirea înregistrărilor**: verificarea semnăturii sau a sigiliului utilizatorului și a conținutului permis (secțiunea 6.3);

– **ordonarea**: atribuirea poziției unice în secvență și legarea criptografică de înregistrarea anterioară, cu marcă temporală calificată (secțiunea 6.4);

– **sigilarea**: aplicarea sigiliului calificat al serviciului pe înregistrări și pe punctele de control (secțiunea 6.5);

– **verificarea și raportarea**: furnizarea automată a dovezilor de includere și a rapoartelor de registru (secțiunile 6.6 și 6.7);

– **păstrarea registrului**: pe toată durata serviciului și la încetarea lui (secțiunile 6.8 și 6.14).

4.2. Arhitectura registrului

Registrul CERTDIGITAL este un **registru centralizat**, creat și administrat numai de CERTDIGITAL, accesibil la https://registru.certdigital.ro. El nu folosește tehnologia registrelor distribuite și nici un mecanism de consens. De aceea, cerințele suplimentare din RE 2025/2531, anexa, pct. 3 lit. (b) (ISO 23257:2022, cl. 9 și ISO/TS 23635:2022) nu se aplică. O înregistrare este finală în momentul în care a fost sigilată și marcată temporal; nu există un interval de așteptare până la finalitate. Registrul și jurnalele sale se replică între centrul de date principal și centrul de date secundar ale CERTDIGITAL.

4.3. Profilul registrului centralizat (47898.13.1.1)

Element	Mecanism
Conținutul înregistrării	amprenta criptografică (SHA-256 sau superioară) a datelor abonatului, tipul înregistrării, identificatorul abonatului și metadatele minime stabilite în contract
Originea	semnătura electronică avansată sau sigiliul electronic avansat al utilizatorului, bazate pe certificat calificat, în format CAdES, XAdES sau JAdES (REQ-7.5-03)
Ordonarea	lanț de amprente: fiecare înregistrare conține amprenta înregistrării anterioare; marcă temporală calificată CERTDIGITAL pe fiecare înregistrare sau pe fiecare punct de control (REQ-7.5-04)
Integritatea	sigiliul electronic calificat al serviciului pe înregistrări și pe punctele de control; orice modificare ulterioară se detectează imediat, prin recalcularea lanțului (REQ-7.5-05)
Finalitatea	la sigilare; înregistrările nu se modifică și nu se șterg

4.4. Datele cu caracter personal în registru

– în registru nu se înscriu date cu caracter personal în clar; se înscriu numai amprente criptografice ale datelor și metadatele strict necesare;

– amprentele datelor care ar putea conține date cu caracter personal se calculează cu o componentă secretă, păstrată de abonat (de exemplu, amprentă cu cheie sau cu valoare aleatoare adăugată), astfel încât datele să nu poată fi deduse sau corelate pornind de la registru, conform Ghidului EDPB 02/2025;

– datele la care se referă amprentele rămân la abonat; exercitarea drepturilor persoanelor vizate (inclusiv ștergerea) se face asupra acestor date, iar înregistrarea din registru devine astfel neasociabilă cu persoana;

– identitatea utilizatorilor din semnăturile sau sigiliile înregistrărilor (certificatele calificate) se păstrează în zona protejată a serviciului și nu se publică în rapoartele publice de verificare.

4.5. Identitatea serviciului și sigiliul serviciului

Înregistrările, punctele de control și rapoartele de registru poartă **sigiliul electronic calificat al serviciului**, creat cu un certificat calificat de sigiliu emis pentru CENTRUL DE CALCUL S.A. și dedicat serviciului, cu cheia păstrată într-un dispozitiv certificat (secțiunea 6.13). Același certificat va identifica serviciul în Lista de încredere a României, după înscriere. Certificatul nu se eliberează abonaților; aceștia folosesc propriile certificate calificate.

Certificatul serviciului este CERTDIGITAL QLEDGERS SERVICE G5, emis de CERTDIGITAL QCA G5, valabil 5 ani, cu cheia RSA 4096 generată în ceremonia cheilor G5 din 23.10.2026, în modulul Thales Luna PCIe HSM 7 A790 (secțiunea 18.2). Profilul lui este descris în DPC CERTDIGITAL G5, secțiunea 7.1.2, iar certificatul se publică la http://certs.certdigital.ro/certdigital_qledgers_g5.crt.

5. Politica serviciului

5.1. Identificare și conformitate

CERTDIGITAL declară conformitatea serviciului cu ETSI EN 319 401 V3.1.1, cu adaptările și cerințele suplimentare din anexa la Regulamentul de punere în aplicare (UE) 2025/2531, ceea ce atrage prezumția de conformitate cu cerințele art. 45l alin. (1) din Regulamentul eIDAS (art. 45l alin. (2)). Conformitatea este evaluată de un organism de evaluare a conformității acreditat (secțiunea 6.15). Pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României (art. 21 din Regulamentul eIDAS); până la înscriere, serviciul nu se prestează ca serviciu de încredere calificat (art. 21 alin. (3)).

5.2. Comunitatea utilizatorilor și aplicabilitatea

Serviciul se adresează persoanelor juridice, autorităților și instituțiilor publice, precum și persoanelor fizice care au nevoie de dovezi cu efect juridic privind existența, originea, ordinea și integritatea unor date, și părților care se bazează pe aceste dovezi.

5.3. Modificarea politicii

Dacă o modificare a prezentului document sau a profilului registrului afectează garanțiile oferite pentru înregistrările existente, identificatorul politicii sau al profilului se schimbă. Înregistrările existente rămân verificabile conform regulilor în vigoare la data înregistrării lor.

6. Cerințele privind practicile

6.1. Publicare și depozit

Prezentul document, termenii și condițiile serviciului (TC-Ledgers), profilul registrului, specificația formatului înregistrărilor și a rapoartelor și certificatul de sigiliu al serviciului sunt publicate la https://www.certdigital.ro/repository/, 24/7, public și fără restricții de acces. Partea a II-a cuprinde cel puțin (RE 2025/2531, REQ-6.1-12):

– capacitățile funcționale și tehnice ale platformei registrului și modul în care este folosită la prestarea serviciului calificat (capitolul 11);

– mecanismele de autentificare a originii datelor (secțiunile 12.3 și 13.3);

– mecanismele de ordonare cronologică secvențială și legătura criptografică folosită (secțiunile 13.4–13.6 și 13.8);

– finalitatea înregistrărilor, registrul nefolosind un mecanism de consens (secțiunea 11.3);

– mecanismele de asigurare a integrității datelor (secțiunile 13.7 și 13.8; capitolul 14).

6.2. Termeni și condiții

Înainte de încheierea contractului, abonații și părțile care se bazează sunt informați, clar, complet și ușor accesibil, atât public, cât și individual, despre termenii și condițiile serviciului, inclusiv despre mecanismele de la secțiunea 6.1, conținutul permis al înregistrărilor, durata păstrării registrului, verificare, răspunderea și limitările ei (RE 2025/2531, REQ-6.2-03).

6.3. Originea înregistrărilor

– fiecare înregistrare este semnată sau sigilată de utilizator cu o semnătură electronică avansată sau un sigiliu electronic avansat, bazate pe certificat calificat, în format CAdES (ETSI EN 319 122-1), XAdES (ETSI EN 319 132-1) sau JAdES (ETSI TS 119 182-1); la JAdES, antetul x5c (lanțul de certificate, RFC 7515) este obligatoriu (RE 2025/2531, REQ-7.5-03);

– la primire, CERTDIGITAL validează semnătura sau sigiliul conform Regulamentului de punere în aplicare (UE) 2025/1945 și verifică dacă utilizatorul este autorizat de abonat; înregistrările care nu trec verificarea se resping, cu motivarea transmisă utilizatorului;

– utilizatorii se autentifică în serviciu prin mijloace de autentificare puternică, cu cel puțin doi factori, sau cu certificat calificat; componentele tehnice ale serviciului și aplicațiile abonatului comunică prin canale autentificate reciproc și criptate.

6.4. Ordonarea cronologică secvențială unică

– fiecare înregistrare primește o poziție unică în secvență și conține amprenta înregistrării anterioare, astfel încât ordinea nu poate fi schimbată fără a rupe lanțul (RE 2025/2531, REQ-7.5-04);

– funcțiile de amprentă folosite sunt SHA-256, SHA3-256 sau superioare, conform ECCG ACM;

– momentul fiecărei înregistrări este stabilit prin **mărci temporale calificate**, emise de serviciul calificat de marcare temporală CERTDIGITAL, aplicate punctelor de control, la cel mult o oră între două puncte; fiecare înregistrare este sigilată și poartă ora UTC a secvențiatorului, iar între două puncte de control ordinea este dată de lanțul de amprente.

6.5. Integritatea și detectarea modificărilor

– CERTDIGITAL asigură integritatea înregistrărilor cu sigiliul electronic calificat al serviciului, aplicat înregistrărilor și punctelor de control (RE 2025/2531, REQ-7.5-05);

– orice modificare ulterioară a unei înregistrări se detectează imediat, prin recalcularea lanțului de amprente și verificarea sigiliilor și a mărcilor temporale (REQ-7.5-05 lit. (d)); CERTDIGITAL verifică automat și continuu consistența registrului și tratează orice neconcordanță ca incident de securitate;

– înregistrările nu se modifică și nu se șterg; o corectură se face printr-o înregistrare nouă, care trimite la înregistrarea corectată.

6.6. Rapoartele de registru

Rapoartele de registru se produc **automat** (RE 2025/2531, anexa, pct. 2), poartă sigiliul calificat al serviciului și o marcă temporală calificată și conțin, după caz: identificatorul și poziția înregistrării, amprenta datelor, momentul înregistrării, dovada de includere în lanț (sau în arborele de amprente) și rezultatul verificării originii. Abonatul poate obține oricând rapoarte privind propriile înregistrări și exportul complet al acestora.

6.7. Verificarea de către părțile care se bazează

Orice parte care se bazează poate verifica gratuit, prin interfața publică a serviciului, dacă o amprentă figurează în registru, poziția și momentul înregistrării ei. Verificarea se poate face și independent, cu datele din raportul de registru și cu certificatele publicate, fără a depinde de disponibilitatea serviciului.

6.8. Păstrarea registrului

– registrul, cu toate înregistrările, punctele de control și dovezile de verificare, se păstrează pe toată durata prestării serviciului și cel puțin 10 ani de la ultima înregistrare a fiecărui abonat;

– dovezile de verificare se reînnoiesc înainte ca algoritmii folosiți să devină nesiguri, conform ECCG ACM, sau înainte de expirarea certificatelor pe care se bazează, fără a modifica înregistrările;

– la expirarea sau la reînnoirea certificatului de sigiliu al serviciului, trecerea la cheia nouă se consemnează în registru printr-un punct de control sigilat cu ambele chei.

6.9. Timpul de încredere și jurnalele

– evenimentele serviciului sunt datate cu o sursă de timp sincronizată cu UTC; mărcile temporale folosite sunt mărci temporale calificate;

– se jurnalizează evenimentele critice și necritice ale serviciului (primiri, respingeri, înregistrări, puncte de control, rapoarte, verificări de consistență, operații administrative, evenimente de securitate), conform ETSI EN 319 401, cl. 7.10; monitorizarea ține seama de sensibilitatea informațiilor colectate (RE 2025/2531, REQ-7.9.1-02X);

– jurnalele se protejează împotriva modificării și se păstrează cel puțin 10 ani.

6.10. Personalul

Personalul cu roluri de încredere este angajat al CENTRUL DE CALCUL S.A. și are cunoștințele, experiența și calificările necesare, dovedite prin instruire formală, atestări sau experiență practică (REQ-7.2-04X), și primește cel puțin o dată la 12 luni instruire privind amenințările noi și practicile de securitate actuale (REQ-7.2-05X).

6.11. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital, cu următoarele precizări:

– serviciul este operat în centrul de date principal și în centrul de date secundar, conform Procedurii DRP (PO_SI_63), cu durata maximă de restabilire de 24 de ore și fără pierderea înregistrărilor confirmate (RPO zero, prin replicarea sincronă din secțiunea 18.8);

– incidentele se notifică conform Procedurii de notificare a incidentelor (00q): ADR în cel mult 24 de ore de la luarea la cunoștință, DNSC, ANSPDCP și persoanele afectate;

– disponibilitatea serviciului este de cel puțin 99,5%, cu excepția intervențiilor planificate anunțate în prealabil.

6.12. Controale criptografice

– cheile, algoritmii și dispozitivele criptografice sunt gestionate pe tot ciclul de viață, cu posibilitatea înlocuirii algoritmilor fără întreruperea serviciului (agilitate criptografică; REQ-7.5-01X);

– tehnicile criptografice respectă ECCG ACM (REQ-7.5-02).

6.13. Protecția cheii serviciului și securitatea rețelei

– cheia privată a sigiliului serviciului se generează, se păstrează și se utilizează numai într-un dispozitiv criptografic certificat Common Criteria EAL4 sau superior, ori EUCC EAL4 sau

superior, ori, până la 31.12.2030, FIPS 140-3 nivel 3, configurat conform certificării (REQ-7.5-06);

– scanarea de vulnerabilități se efectuează cel puțin o dată pe trimestru (REQ-7.8-14X), testul de penetrare cel puțin o dată pe an (REQ-7.8-18X), iar firewall-urile blochează toate protocoalele și accesele care nu sunt necesare funcționării serviciului (REQ-7.8-21X).

6.14. Notificări către ADR și încetarea serviciului

– CERTDIGITAL notifică ADR orice modificare a prestării serviciului cu cel puțin **o lună** înainte de aplicare și intenția de încetare cu cel puțin **trei luni** înainte (RE 2025/2531, REQ-6.3-04X);

– încetarea serviciului se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530 (REQ-7.12-02A): registrul, punctele de control, dovezile de verificare și jurnalele se transferă unui alt prestator calificat de registre electronice acceptat de ADR, iar abonații primesc exportul complet al înregistrărilor lor; registrul rămâne verificabil după încetare, cu certificatele și specificațiile publicate.

6.15. Evaluarea conformității

Serviciul este evaluat de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162, cel puțin o dată la 24 de luni (art. 20 din Regulamentul eIDAS); ADR este informată cu cel puțin o lună înainte, iar raportul se transmite ADR în cel mult 3 zile lucrătoare. CERTDIGITAL efectuează anual un audit intern.

7. Obligații și răspundere

7.1. Obligațiile CERTDIGITAL

– creează și administrează registrul conform art. 45l alin. (1): stabilește originea înregistrărilor, le ordonează cronologic secvențial unic și le înregistrează astfel încât orice modificare ulterioară să fie detectată imediat;

– nu modifică și nu șterge înregistrările;

– furnizează automat rapoartele de registru și permite verificarea publică gratuită;

– păstrează registrul conform secțiunii 6.8 și îl transferă la încetarea serviciului;

– publică documentația serviciului 24/7.

7.2. Obligațiile abonatului și ale utilizatorilor

– nu înscriu în registru date cu caracter personal în clar și calculează amprentele datelor sensibile conform secțiunii 4.4;

– semnează sau sigilează înregistrările numai cu certificate calificate valabile și păstrează sub control exclusiv cheile și mijloacele de autentificare;

– păstrează datele la care se referă amprentele, deoarece serviciul nu le stochează;

– utilizează serviciul numai în scopuri legale, conform termenilor și condițiilor.

7.3. Obligațiile părților care se bazează

Verifică sigiliul calificat și marca temporală calificată de pe înregistrare sau de pe raportul de registru și statutul calificat al serviciului în Lista de încredere a României.

7.4. Răspunderea

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

CERTDIGITAL nu răspunde pentru prejudiciile rezultate din: conținutul și exactitatea datelor la care se referă amprentele; pierderea acestor date de către abonat; utilizarea serviciului peste limitările notificate în prealabil și recognoscibile de terți; nerespectarea de către abonat sau utilizatori a obligațiilor de la secțiunea 7.2; neverificarea de către partea care se bazează a sigiliului, a mărcii temporale și a statutului din Lista de încredere; forța majoră. Nicio prevedere nu exclude și nu limitează răspunderea pentru intenție sau culpă gravă (art. 1355 Cod civil); în raporturile cu consumatorii se aplică Legea nr. 193/2000.

7.5. Asigurarea

CENTRUL DE CALCUL S.A. deține, pentru serviciul de registre electronice calificate, o poliță distinctă de asigurare de răspundere civilă profesională, cu limita răspunderii de 500.000 EUR pe perioada asigurată, în condițiile art. 24 alin. (2) lit. c) din Regulamentul eIDAS și ale art. 5 alin. (2) lit. b) din procedura aprobată prin Ordinul MEDAT nr. 102/2026; în poliță, ADR, în calitate de organism de supraveghere, are calitatea de asigurat adițional. Polița se reînnoiește înainte de expirare; datele ei de identificare (asigurătorul, seria și numărul, perioada de valabilitate) sunt comunicate ADR și se pun la dispoziție la cerere.

8. Alte aspecte comerciale și juridice

8.1. Tarife

Tarifele serviciului sunt cele din lista de tarife publicată pe site-ul https://www.certdigital.ro/ sau cele din oferta transmisă la cerere (art. 11 alin. (1) din Legea nr. 214/2024). Verificarea publică a înregistrărilor este gratuită.

8.2. Protecția datelor cu caracter personal

Pentru datele înregistrate de abonați, CERTDIGITAL acționează în calitate de **persoană împuternicită** a abonatului (art. 28 din Regulamentul (UE) 2016/679), pe baza clauzelor din contract; pentru datele de identificare, de cont, pentru datele din certificatele utilizatorilor și pentru jurnalele serviciului, CERTDIGITAL este **operator**, conform Politicii de protecție a datelor (00d). Arhitectura serviciului aplică principiul protecției datelor începând cu momentul conceperii (art. 25 GDPR) prin regulile de la secțiunea 4.4. CERTDIGITAL nu folosește persoane împuternicite pentru operarea serviciului. Responsabilul cu protecția datelor: dpo@centruldecalcul.ro.

8.3. Modificări

Orice modificare a prezentului document primește o versiune nouă, aprobată de Directorul General și publicată în depozitul de documente; versiunile anterioare rămân disponibile. Modificările care afectează prestarea serviciului se comunică ADR cu cel puțin o lună înainte de aplicare (cu cel puțin trei luni în cazul încetării serviciului). Abonații și părțile care se bazează sunt informați prin publicare pe site cu cel puțin 30 de zile înainte de intrarea în vigoare. Corecturile de redactare care nu modifică drepturile sau obligațiile părților se publică cu versiune nouă, fără termen de preaviz.

8.4. 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).

8.5. Legea aplicabilă și cadrul legal

Prezentul document și raporturile juridice decurgând din furnizarea serviciului sunt guvernate de dreptul român, sub rezerva dispozițiilor direct aplicabile ale dreptului Uniunii Europene. Serviciul este furnizat în conformitate cu actele normative de la secțiunea 2.1. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

8.6. Alte prevederi

Abonatul păstrează toate drepturile asupra datelor sale; CERTDIGITAL dobândește numai dreptul de a prelucra înregistrările în măsura necesară prestării serviciului. CERTDIGITAL urmărește accesibilitatea serviciilor pentru persoanele cu dizabilități (art. 15 din Regulamentul eIDAS); persoanele cu dizabilități pot solicita asistență prin telefon, e-mail sau la sediu.

9. Corespondența cu cerințele Regulamentului (UE) 2025/2531

9.1. Tabel de corespondență

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 45k alin. (2)	prezumția ordonării cronologice secvențiale unice și exacte și prezumția de integritate	1.1
Regulamentul eIDAS, art. 45l alin. (1) lit. (a)	creat și administrat de un prestator calificat	1.3, 4.2, 5.1
Regulamentul eIDAS, art. 45l alin. (1) lit. (b)	originea înregistrărilor	4.3, 6.3
Regulamentul eIDAS, art. 45l alin. (1) lit. (c)	ordonarea cronologică secvențială unică	4.3, 6.4
Regulamentul eIDAS, art. 45l alin. (1) lit. (d)	detectarea imediată a modificărilor; integritatea în timp	6.5, 6.8
RE 2025/2531, anexa, pct. 1	definiții (finalitate, legătură criptografică, raport de registru)	3.1
RE 2025/2531, anexa, pct. 2	rapoarte de registru produse automat	6.6
REQ-6.1-12	conținutul declarației de practici a registrului	1.1, 6.1
REQ-6.2-03	termeni și condiții publici și individuali	6.2
REQ-6.3-04X	notificări ADR (o lună / trei luni)	6.14, 8.3
REQ-7.2-04X, REQ-7.2-05X	personal; instruire la 12 luni	6.10
REQ-7.5-01X, REQ-7.5-02	gestionarea criptografiei; agilitate; ECCG ACM	6.12
REQ-7.5-03	originea prin AdES pe certificat calificat (CAdES, XAdES, JAdES cu x5c)	6.3
REQ-7.5-04	lanț sau arbore de amprente SHA-256 / SHA3-256; mărci temporale calificate	6.4
REQ-7.5-05	integritate prin sigiliu pe certificat calificat; detectare imediată	6.5
REQ-7.5-06	cheia prestatorului în dispozitiv certificat (CC / EUCC EAL4+, FIPS 140-3 nivel 3 până la 31.12.2030)	4.5, 6.13
REQ-7.8-14X, 7.8-18X, 7.8-21X	scanare trimestrială; test de penetrare anual; firewall	6.13
REQ-7.9.1-02X	monitorizarea ține seama de sensibilitatea informațiilor	6.9
REQ-7.12-02A	plan de încetare conform 2025/2530	6.14
RE 2025/2531, anexa, pct. 3 lit. (b)	ISO 23257 / ISO/TS 23635 — numai pentru DLT; nu se aplică	2.1, 4.2
Ghidul EDPB 02/2025	fără date personale în clar; amprente cu componentă secretă	4.4, 8.2

Practicile detaliate pentru fiecare cerință sunt descrise în Partea a II-a; corespondența lor cu cerințele este în anexa A.

PARTEA A II-A – Declarația de practici

10. Publicare și depozit

Partea a II-a descrie modul în care CERTDIGITAL îndeplinește cerințele din Partea I și din Regulamentul de punere în aplicare (UE) 2025/2531. Identificarea documentului, participanții, referințele normative, definițiile și acronimele sunt cele din Partea I (capitolele 1–3). Corespondența practicilor cu cerințele și cu secțiunile Părții I este în anexa A.

10.1. Documentele și informațiile publicate

La https://www.certdigital.ro/repository/ se publică, 24/7, public și fără restricții de acces (secțiunea 6.1):

– prezentul document și termenii și condițiile serviciului (TC-Ledgers);

– specificația formatului înregistrărilor, al confirmărilor, al dovezilor de includere, al punctelor de control și al rapoartelor de registru, cu algoritmii folosiți și cu pașii verificării independente (secțiunea 14.3);

– specificația interfeței de programare a serviciului, cu lista codurilor de respingere (secțiunea 13.10);

– ghidul pentru abonați privind calculul amprentelor cu componentă secretă (secțiunea 13.1);

– certificatul calificat de sigiliu al serviciului, lanțul lui de certificare și certificatele unităților de marcare temporală folosite de serviciu;

– atestarea de conformitate emisă de organismul de evaluare a conformității (secțiunea 18.13);

– tarifele (secțiunea 8.1).

Lista punctelor de control se publică pe interfața publică de verificare (secțiunea 13.8). Versiunile anterioare ale documentelor rămân disponibile în depozit.

10.2. Informarea abonaților și a părților care se bazează

Termenii și condițiile serviciului se publică în depozitul de documente și se transmit individual fiecărui solicitant, pe un suport durabil, înainte de încheierea contractului (secțiunea 6.2; RE 2025/2531, REQ-6.2-03). Ei cuprind informațiile cerute de ETSI EN 319 401, cl. 6.2, mecanismele de la secțiunea 6.1, conținutul permis al înregistrărilor, durata păstrării registrului, modul de verificare, răspunderea și limitările ei. Acceptarea termenilor și condițiilor se consemnează la încheierea contractului. Părțile care se bazează găsesc aceleași informații în depozitul de documente.

10.3. Revizuirea și modificarea documentului

Prezentul document se revizuiește cel puțin o dată pe an și la orice schimbare a serviciului, a platformei registrului sau a cerințelor aplicabile. Modificările se aprobă de Directorul General, se

publică și se comunică conform secțiunii 8.3: ADR este notificată cu cel puțin o lună înainte de aplicarea oricărei modificări a prestării serviciului și cu cel puțin trei luni înainte de încetarea planificată a serviciului (RE 2025/2531, REQ-6.3-04X).

11. Platforma registrului

11.1. Capacitățile funcționale

Platforma registrului asigură funcțiile de mai jos, folosite pe toată durata prestării serviciului calificat (RE 2025/2531, REQ-6.1-12):

Funcția	Ce face	Secțiunea
Primirea	primește înregistrările prin interfața de programare sau prin portalul abonatului și verifică formatul, autorizarea utilizatorului și semnătura sau sigiliul acestuia	13.1–13.3
Ordonarea	atribuie fiecărei înregistrări acceptate următoarea poziție din secvență și o leagă criptografic de înregistrarea anterioară	13.4, 13.5
Marcarea temporală	obține mărci temporale calificate pentru înregistrări sau pentru punctele de control	13.6
Sigilarea	aplică sigiliul calificat al serviciului pe înregistrări, pe punctele de control și pe rapoartele de registru	13.7
Punctele de control	fixează periodic starea registrului, o sigilează, o marchează temporal și o publică	13.8
Confirmarea și respingerea	transmite utilizatorului confirmarea înregistrării sau motivul respingerii	13.9, 13.10
Verificarea și raportarea	furnizează dovezile de includere, rapoartele de registru și verificarea publică	14
Exportul	furnizează abonatului exportul complet al înregistrărilor sale	16.4
Monitorizarea	verifică automat și continuu consistența registrului și jurnalizează evenimentele	17.3, 17.4
Administrarea	gestionează abonații, utilizatorii autorizați și configurația, fără vreo funcție de modificare sau de ștergere a înregistrărilor	12, 15.1, 17.1

11.2. Arhitectura tehnică

– registrul este centralizat, creat și administrat numai de CERTDIGITAL și accesibil la adresa de la secțiunea 4.2; el nu are noduri externe și nu folosește tehnologia registrelor distribuite;

– platforma are următoarele componente: interfața de primire (API și portal), componenta de validare a semnăturilor și sigiliilor, secvențiatorul, componenta de sigilare, legată de modulele criptografice hardware (secțiunea 18.2), clientul de marcare temporală, depozitul registrului, interfața publică de verificare și componenta de monitorizare a consistenței;

– secvențiatorul este singura componentă care poate adăuga înregistrări; el funcționează într-o singură instanță activă, astfel încât în registru nu pot exista două secvențe paralele (secțiunea 13.4);

– depozitul registrului permite numai adăugarea la sfârșitul secvenței; înregistrările scrise nu se mai actualizează și nu se șterg (secțiunea 15.1);

– registrul, punctele de control și jurnalele se replică în centrul de date secundar (secțiunile 4.2 și 18.8);

– componentele comunică între ele și cu aplicațiile abonaților prin canale TLS autentificate reciproc, conform ECCG ACM (secțiunea 6.3).

11.3. Finalitatea înregistrărilor

– registrul nu folosește un mecanism de consens; cerințele din RE 2025/2531, anexa, pct. 3 lit. (b) nu se aplică (secțiunea 4.2);

– o înregistrare devine finală, adică ireversibilă (RE 2025/2531, anexa, pct. 1 lit. (a)), în momentul în care a fost sigilată de serviciu și marcată temporal calificat (secțiunile 4.2 și 4.3); nu există un interval de așteptare până la finalitate;

– după finalitate, înregistrarea nu mai poate fi modificată sau eliminată; corecturile se fac numai prin înregistrări noi (capitolul 15).

O înregistrare devine finală la sigilarea ei de către serviciu; punctul de control marcat temporal care o include confirmă ulterior momentul înscrierii (secțiunea 6.4).

12. Accesul la serviciu

12.1. Contractul și contul abonatului

– serviciul se furnizează pe bază de contract, încheiat după informarea solicitantului (secțiunea 10.2);

– la încheierea contractului, CERTDIGITAL identifică abonatul și persoana care îl reprezintă: pentru persoanele juridice, pe baza datelor din registrul comerțului sau din registrul echivalent și a împuternicirii reprezentantului; pentru persoanele fizice, pe baza actului de identitate prezentat la sediu sau a semnăturii electronice calificate aplicate pe contract;

– contractul stabilește tipurile de înregistrări, metadatele permise (secțiunea 4.3), administratorul contului desemnat de abonat, durata păstrării registrului (secțiunea 6.8) și clauzele privind prelucrarea datelor în numele abonatului (secțiunea 8.2);

– abonatul primește un cont, în care administratorul desemnat gestionează utilizatorii autorizați (secțiunea 12.2) și obține rapoartele și exportul (secțiunile 14.5 și 16.4).

12.2. Utilizatorii autorizați

– administratorul contului înscrie fiecare utilizator autorizat, cu datele de identificare și cu certificatul calificat de semnătură sau de sigiliu pe care acesta îl folosește pentru înregistrări; pentru sigilii, abonatul indică certificatele de sigiliu și sistemele informatice care le folosesc;

– serviciul acceptă înregistrări numai de la utilizatorii înscriși și activi la momentul primirii (secțiunea 6.3);

– administratorul poate suspenda sau retrage oricând un utilizator; modificarea produce efecte din momentul consemnării ei în cont, se jurnalizează și nu afectează înregistrările anterioare;

– abonatul menține lista utilizatorilor autorizați actualizată, conform termenilor și condițiilor serviciului.

12.3. Autentificarea

Situația	Mijloace acceptate
Utilizator sau administrator al abonatului, în portal	autentificare cu doi factori sau cu certificat calificat
Aplicație sau sistem informatic al abonatului, prin API	TLS cu autentificare reciprocă, cu certificat emis pentru abonat, și cheie de acces asociată contului
Parte care se bazează, pe interfața publică de verificare	fără autentificare
Personalul CERTDIGITAL	conform secțiunii 17.1

Autentificarea în serviciu nu înlocuiește semnătura sau sigiliul utilizatorului pe fiecare înregistrare (secțiunea 13.3). Încercările de autentificare eșuate se jurnalizează, iar contul se blochează temporar după depășirea unui prag.

Utilizatorii se autentifică cu doi factori, iar aplicațiile abonaților prin autentificare reciprocă TLS, cu certificate emise pentru acestea. Dimensiunea maximă a unei înregistrări și numărul de cereri pe unitatea de timp se stabilesc prin contract.

12.4. Interfața de programare

Interfața de programare a serviciului permite: transmiterea unei înregistrări și primirea confirmării; obținerea dovezii de includere și a punctului de control; obținerea rapoartelor de registru; exportul înregistrărilor abonatului; verificarea unei amprente. Operațiile, formatele, codurile de respingere și limitele sunt descrise în specificația publicată (secțiunea 10.1). Adresa punctului de acces este cea de la secțiunea 4.2.

13. Înregistrarea datelor

13.1. Datele acceptate

– fiecare înregistrare conține amprenta datelor abonatului, calculată de abonat cu una dintre funcțiile SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384 sau SHA3-512, conform ECCG ACM; serviciul nu primește datele la care se referă amprenta;

– înregistrarea mai conține tipul ei, ales din lista stabilită în contract, și metadatele permise de contract, verificate de serviciu după tip, lungime și format; câmpurile care nu sunt prevăzute în contract se resping;

– în registru nu se înscriu date cu caracter personal în clar (secțiunea 4.4); amprentele datelor care ar putea conține date cu caracter personal se calculează cu componentă secretă, după ghidul publicat de CERTDIGITAL (secțiunea 10.1); serviciul nu poate verifica dacă o amprentă a fost calculată astfel, iar respectarea regulii revine abonatului (secțiunea 7.2);

– limitele de dimensiune sunt cele din specificația interfeței (secțiunea 12.4).

13.2. Structura înregistrării

Câmp	Conținut	Stabilit de
Identificatorul înregistrării	identificator unic, care nu se refolosește	serviciu
Poziția	numărul de ordine în secvența registrului (secțiunea 13.4)	serviciu
Profilul	1.3.6.1.4.1.47898.13.1.1	serviciu
Abonatul	identificatorul intern al contului abonatului, fără numele sau denumirea acestuia	serviciu
Tipul înregistrării și, la corecturi, trimiterea la înregistrarea corectată	conform contractului (secțiunea 15.2)	utilizator
Amprenta datelor	valoarea amprentei și identificatorul funcției folosite	utilizator
Metadatele	numai cele permise de contract, fără date cu caracter personal în clar	utilizator
Semnătura sau sigiliul utilizatorului	AdES pe certificat calificat, asupra câmpurilor stabilite de utilizator (secțiunea 13.3); se păstrează în zona protejată (secțiunea 4.4)	utilizator
Momentul primirii	data și ora (UTC), din sursa de timp sincronizată (secțiunea 13.4)	serviciu
Legătura cu înregistrarea anterioară	amprenta înregistrării anterioare și identificatorul funcției de amprentă (secțiunea 13.5)	serviciu
Sigiliul serviciului	sigiliul calificat al serviciului, asupra tuturor câmpurilor de mai sus (secțiunea 13.7)	serviciu
Marca temporală calificată	asupra sigiliului serviciului, dacă se marchează temporal fiecare înregistrare (secțiunea 13.6)	serviciu

Înregistrările, confirmările și dovezile de includere sunt structuri JSON sigilate în format JAdES, cu antetul x5c, iar rapoartele lizibile sunt documente PDF sigilate în format PAdES. Dovada de includere este lanțul de amprente, completat cu un arbore de amprente (Merkle) pentru fiecare punct de control. Metadatele și semnătura utilizatorului intră în lanț prin amprenta lor (secțiunea 15.4).

13.3. Verificarea originii

– utilizatorul semnează sau sigilează câmpurile înregistrării pe care le stabilește (tipul, amprenta datelor, metadatele, trimiterea la înregistrarea corectată) cu propriul certificat calificat, în format CAdES (ETSI EN 319 122-1), XAdES (ETSI EN 319 132-1) sau JAdES (ETSI TS 119 182-1) cu antetul x5c, în profilul de bază al standardului respectiv (RE 2025/2531, REQ-7.5-03);

– la primire, serviciul validează semnătura sau sigiliul conform Regulamentului de punere în aplicare (UE) 2025/1945 și ETSI EN 319 102-1: integritatea criptografică; lanțul de certificare până la o ancoră de încredere din listele de încredere ale statelor membre; caracterul calificat al certificatului, pentru semnătură sau pentru sigiliu; starea certificatului la momentul primirii, prin OCSP sau CRL; conformitatea algoritmilor cu ECCG ACM;

– serviciul verifică apoi că certificatul aparține unui utilizator autorizat și activ al abonatului (secțiunea 12.2);

– dacă starea certificatului nu poate fi stabilită la momentul primirii, înregistrarea se respinge cu un cod de eroare temporară, iar utilizatorul o poate retransmite;

– rezultatul verificării originii și datele de validare folosite (certificatele și informațiile de revocare) se păstrează împreună cu înregistrarea, în zona protejată, și se includ în rapoartele de registru (secțiunile 14.5 și 16.2).

Validarea semnăturilor și a sigiliilor se face prin serviciul calificat de validare CERTDIGITAL (PDP-QESVal).

13.4. Ordonarea cronologică secvențială unică

– registrul este o singură secvență, comună tuturor abonaților; ordinea înregistrărilor unui abonat este dată de pozițiile lor în această secvență;

– secvențiatorul adaugă înregistrările acceptate una câte una, în ordinea încheierii verificărilor de la secțiunea 13.3; fiecare înregistrare primește poziția următoare celei a ultimei înregistrări sigilate, astfel încât pozițiile sunt strict crescătoare, fără goluri și fără repetări (RE 2025/2531, REQ-7.5-04);

– adăugarea este atomică: poziția, legătura cu înregistrarea anterioară și sigiliul serviciului se stabilesc într-o singură operație; o operație întreruptă nu ocupă nicio poziție;

– momentul primirii se stabilește din sursa de timp a CERTDIGITAL, sincronizată cu UTC (00u), și nu scade de la o poziție la următoarea; dacă sincronizarea se pierde, serviciul suspendă primirea înregistrărilor până la restabilirea ei (secțiunea 18.10);

– momentul calificat al înregistrărilor este stabilit prin mărcile temporale calificate (secțiunea 13.6).

13.5. Legătura criptografică

– fiecare înregistrare conține amprenta înregistrării anterioare, calculată asupra întregii înregistrări sigilate; prima înregistrare a registrului conține o valoare inițială fixă, publicată în specificație;

– funcția de amprentă a lanțului este SHA-256 sau superioară, conform ECCG ACM (secțiunea 6.4); identificatorul ei se înscrie în fiecare înregistrare, astfel încât funcția poate fi schimbată fără ruperea lanțului, printr-un punct de control (secțiunea 18.3);

– legătura face ca nicio înregistrare să nu poată fi inserată, eliminată, modificată sau mutată fără ruperea lanțului în acel punct, ceea ce se constată la orice verificare (secțiunile 14.4 și 17.4);

– dovada de includere a unei înregistrări într-un punct de control se obține din lanțul de amprente dintre cele două sau, dacă se folosește un arbore de amprente, din calea de amprente până la rădăcina lui (secțiunea 14.1).

13.6. Mărcile temporale calificate

– mărcile temporale calificate se obțin de la serviciul calificat de marcare temporală al CERTDIGITAL (PDP-QTST), prin protocolul IETF RFC 3161, cu profilul ETSI EN 319 422; ele se aplică fiecărui punct de control și, dacă se decide astfel, fiecărei înregistrări (secțiunea 6.4);

– marca temporală se aplică asupra sigiliului serviciului (nivelul B-T), deci acoperă înregistrarea sau punctul de control sigilat;

– înainte de folosire, serviciul verifică marca temporală primită: sigiliul unității de marcare temporală, valabilitatea certificatului ei, amprenta acoperită și diferența față de ora proprie;

– dacă marca temporală nu poate fi obținută, serviciul reîncearcă; dacă nu o obține în intervalul maxim dintre două puncte de control (secțiunea 6.4), suspendă primirea înregistrărilor noi până la restabilire și tratează evenimentul ca incident (secțiunea 18.10).

Unitatea de marcare temporală folosită de serviciu este CERTDIGITAL TSA G5.

13.7. Sigilarea cu sigiliul calificat al serviciului

– fiecare înregistrare acceptată se sigilează cu sigiliul electronic calificat al serviciului imediat după ordonare și înainte de transmiterea confirmării; sigiliul acoperă toate câmpurile

înregistrării, inclusiv poziția și legătura cu înregistrarea anterioară (RE 2025/2531, REQ-7.5-05);

– sigiliul este un sigiliu electronic calificat (deci și avansat), creat cu o cheie păstrată într-un dispozitiv calificat (secțiunea 18.2) și bazat pe certificatul calificat de sigiliu al serviciului (secțiunea 4.5), care conține declarația QcSSCD, cu funcție de amprentă SHA-256, SHA3-256 sau superioară și cu algoritmi conformi cu ECCG ACM (REQ-7.5-05 lit. (a)–(c)); înregistrările se sigilează cel puțin la nivelul B-B (B-T, dacă se marchează temporal fiecare înregistrare), iar punctele de control și rapoartele de registru, la nivelul B-T;

– înainte de sigilare, componenta de sigilare verifică faptul că legătura înregistrării corespunde ultimei înregistrări sigilate; în caz contrar, refuză sigilarea și semnalează incidentul (secțiunea 15.3);

– cheia sigiliului se folosește numai pentru înregistrări, puncte de control și rapoarte de registru (secțiunea 18.2).

13.8. Punctele de control și ancorarea lor

– punctul de control cuprinde: poziția ultimei înregistrări incluse, amprenta acesteia (capul lanțului) sau rădăcina arborelui de amprente, numărul de înregistrări, amprenta punctului de control anterior și momentul emiterii; el se sigilează cu sigiliul serviciului și se marchează temporal calificat;

– punctele de control se emit la intervalul stabilit la secțiunea 6.4 și, în plus, la schimbarea cheii serviciului (secțiunea 16.3), la schimbarea unui algoritm (secțiunea 18.3), înainte și după intervențiile planificate, la reînnoirea dovezilor (secțiunea 16.2) și la încetarea serviciului (secțiunea 16.5);

– fiecare punct de control se publică imediat pe interfața publică de verificare, într-o listă la care se poate numai adăuga; oricine îl poate descărca și păstra, iar abonații îl primesc și în rapoartele de registru;

– publicarea face ca nici CERTDIGITAL să nu poată rescrie istoricul registrului fără ca diferența să fie constatată de cei care au păstrat punctele de control anterioare (secțiunea 14.4).

Punctele de control se păstrează suplimentar prin serviciul de păstrare CERTDIGITAL (QPS, profilul WOS).

13.9. Confirmarea înregistrării

După sigilare, utilizatorul primește confirmarea înregistrării: înregistrarea sigilată, cu identificatorul, poziția, amprenta ei, amprenta înregistrării anterioare, momentul primirii și, dacă se aplică, marca temporală calificată. După emiterea primului punct de control care include înregistrarea, dovada de includere și punctul de control se pot obține prin interfața de programare

sau din cont (secțiunea 14.1). Confirmările rămân disponibile abonatului pe toată durata păstrării registrului.

13.10. Respingerea înregistrărilor

O înregistrare se respinge dacă:

– formatul, tipul sau metadatele nu corespund specificației ori contractului;

– funcția de amprentă nu este acceptată (secțiunea 13.1);

– semnătura sau sigiliul utilizatorului nu este valid, nu se bazează pe un certificat calificat sau certificatul este expirat ori revocat la momentul primirii;

– starea certificatului nu poate fi stabilită (eroare temporară, secțiunea 13.3);

– utilizatorul nu este autorizat sau contul abonatului este suspendat;

– sunt depășite limitele de utilizare (secțiunea 12.3) ori primirea este suspendată (secțiunile 13.4 și 13.6).

Răspunsul conține codul motivului, din lista publicată în specificația interfeței. Înregistrarea respinsă nu primește poziție în registru; respingerea se jurnalizează (secțiunea 17.3).

14. Verificarea de către părțile care se bazează

14.1. Dovezile puse la dispoziție

Dovada	Conținut	Cine o obține
Confirmarea înregistrării	înregistrarea sigilată (secțiunea 13.9)	utilizatorul și abonatul
Dovada de includere	amprentele care leagă înregistrarea de un punct de control (secțiunea 13.5)	abonatul, prin API sau din cont; părțile care se bazează, de la abonat sau prin interfața publică
Punctul de control	starea registrului, sigilată și marcată temporal calificat (secțiunea 13.8)	oricine, pe interfața publică
Raportul de registru	informațiile verificabile extrase din registru, sigilate și marcate temporal calificat (secțiunea 14.5)	abonatul, oricând; părțile care se bazează, de la abonat sau, pentru informațiile publice, prin interfața publică

14.2. Verificarea prin interfața publică

– verificarea este gratuită și nu necesită cont (secțiunea 8.1);

– partea care se bazează introduce amprenta datelor pe care le deține și, dacă îl cunoaște, identificatorul înregistrării; interfața răspunde dacă amprenta figurează în registru și, în caz afirmativ, cu poziția și momentul înregistrării, punctul de control care o include, dovada de includere și un raport de registru sigilat cu aceste informații (secțiunea 6.7);

– interfața nu afișează identitatea abonatului sau a utilizatorului, metadatele și nici semnătura sau sigiliul utilizatorului (secțiunea 4.4); ea răspunde numai la căutări după amprenta exactă și limitează numărul de interogări, pentru a împiedica enumerarea registrului;

– pentru amprentele calculate cu componentă secretă, verificarea se face cu amprenta comunicată de abonat sau recalculată cu componenta secretă primită de la acesta.

14.3. Verificarea independentă

Verificarea nu depinde de disponibilitatea serviciului (secțiunea 6.7). Cu confirmarea sau cu raportul de registru, cu certificatele publicate și cu specificația de la secțiunea 10.1, partea care se bazează:

– recalculează amprenta datelor pe care le deține, cu componenta secretă primită de la abonat, dacă este cazul, și o compară cu amprenta din înregistrare;

– verifică sigiliul serviciului pe înregistrare și faptul că certificatul lui este certificatul calificat al serviciului, înscris în Lista de încredere a României pentru serviciul Ledgers/Q, folosind orice instrument de validare conform ETSI EN 319 102-1;

– verifică, dacă originea este relevantă, semnătura sau sigiliul utilizatorului și rezultatul verificării originii din raportul de registru;

– recalculează dovada de includere, de la înregistrare până la punctul de control;

– verifică sigiliul și marca temporală calificată ale punctului de control;

– compară, opțional, punctul de control cu lista publicată sau cu copiile păstrate anterior.

Dacă toți pașii reușesc, înregistrarea se afla în registru, în poziția indicată, cel târziu la momentul mărcii temporale calificate a punctului de control (sau al propriei mărci temporale calificate) și nu a fost modificată de atunci.

14.4. Verificarea ordinii și a integrității

– ordinea a două înregistrări este dată de pozițiile lor; ea se dovedește prin lanțul de amprente dintre ele sau prin includerea lor în același punct de control ori în puncte de control succesive;

– marca temporală calificată a primului punct de control care include o înregistrare (sau propria marcă temporală calificată) dovedește că înregistrarea exista la acel moment; momentul primirii, înscris de serviciu, îl precizează în intervalul dintre două puncte de control;

– orice modificare a unei înregistrări îi schimbă amprenta, ceea ce rupe legătura cu înregistrarea următoare, invalidează sigiliul și dovada de includere și se detectează imediat, la orice verificare (RE 2025/2531, REQ-7.5-05 lit. (d));

– consistența dintre două puncte de control se dovedește prin lanțul care le leagă: punctul de control ulterior conține, prin amprenta punctului anterior și prin lanț, întreaga stare fixată de acesta; CERTDIGITAL furnizează această dovadă în raportul de consistență (secțiunea 14.5).

14.5. Rapoartele de registru

– rapoartele de registru se produc automat de platformă, fără intervenție manuală asupra conținutului (RE 2025/2531, anexa, pct. 2), și poartă sigiliul calificat al serviciului și o marcă temporală calificată (secțiunea 6.6);

– tipurile de rapoarte sunt: raportul înregistrării (înregistrarea, rezultatul verificării originii, dovada de includere și punctul de control), raportul abonatului (înregistrările abonatului dintr-o perioadă, cu dovezile lor) și raportul de consistență (legătura dintre două puncte de control);

– rapoartele se furnizează într-un format prelucrabil automat și într-un format lizibil, conform specificației publicate (secțiunea 10.1);

– abonatul obține oricând rapoarte privind propriile înregistrări; raportul public de verificare (secțiunea 14.2) cuprinde numai informațiile publice.

15. Corecturi și imuabilitate

15.1. Imuabilitatea registrului

– registrul permite numai adăugarea de înregistrări; nici interfața de programare, nici portalul și nici instrumentele de administrare nu au funcții de modificare sau de ștergere a înregistrărilor (secțiunea 6.5);

– drepturile asupra depozitului registrului sunt configurate astfel încât nicio componentă și niciun rol să nu poată actualiza sau șterge înregistrările scrise; orice încercare se jurnalizează;

– dacă aceste măsuri ar fi ocolite, modificarea ar fi detectată imediat prin lanțul de amprente, prin sigilii și prin punctele de control publicate (secțiunile 14.4 și 17.4);

– după o restaurare din copii de rezervă, consistența registrului se verifică față de ultimul punct de control publicat, înainte de reluarea primirii înregistrărilor (secțiunea 18.8).

15.2. Corecturile

– o înregistrare greșită nu se modifică și nu se șterge; corectura se face printr-o înregistrare nouă, de tip „corectură”, care conține identificatorul și amprenta înregistrării corectate și este semnată sau sigilată de un utilizator autorizat al aceluiași abonat (secțiunea 6.5);

– în același mod, abonatul poate declara printr-o înregistrare nouă, de tip „anulare”, că o înregistrare anterioară nu mai produce efecte în procesele sale;

– înregistrarea corectată rămâne în registru; rapoartele de registru indică, pentru fiecare înregistrare, corecturile și anulările care trimit la ea.

15.3. Neconcordanțele și erorile de operare

– dacă verificarea continuă (secțiunea 17.4) sau o parte care se bazează constată o neconcordanță (legătură ruptă, sigiliu nevalid, diferență față de un punct de control publicat), serviciul suspendă primirea înregistrărilor și tratează neconcordanța ca incident de securitate (secțiunile 6.5 și 18.10);

– registrul nu se rescrie; după investigație, se stabilește partea din registru confirmată de punctele de control valide publicate, iar constatările și măsurile luate se consemnează într-o înregistrare nouă, de tip „incident”, sigilată de serviciu;

– abonații ale căror înregistrări sunt afectate și ADR sunt informați conform secțiunii 18.10.

15.4. Datele cu caracter personal

– registrul nu conține date cu caracter personal în clar (secțiunea 4.4); dreptul la ștergere al persoanei vizate se exercită asupra datelor păstrate de abonat și asupra componentei secrete, după care înregistrarea nu mai poate fi asociată cu persoana (Ghidul EDPB 02/2025);

– semnăturile și certificatele utilizatorilor se păstrează în zona protejată a serviciului, accesibilă numai abonatului și rolurilor de încredere care au nevoie de ele, și nu se publică (secțiunea 17.2);

– dacă un abonat înscrie totuși date cu caracter personal în clar, CERTDIGITAL îl informează și restricționează accesul la înregistrarea respectivă până la stabilirea măsurilor, împreună cu abonatul, în calitatea acestuia de operator.

Lanțul și sigiliul serviciului acoperă metadatele și semnătura utilizatorului prin amprenta lor (secțiunea 13.2). Conținutul acestora, inclusiv datele cu caracter personal înscrise din eroare în clar și, la sfârșitul perioadei de păstrare, semnăturile și certificatele utilizatorilor, se poate elimina din zona protejată fără ruperea lanțului; eliminarea se consemnează printr-o înregistrare nouă.

16. Păstrarea, exportul și predarea registrului

16.1. Durata păstrării

Ce se păstrează	Cât	Observații
Înregistrările, punctele de control și dovezile de includere	pe toată durata prestării serviciului și cel puțin durata de la secțiunea 6.8	nu se șterg; după încetarea contractului, înregistrările abonatului rămân în registru
Semnăturile și certificatele utilizatorilor, rezultatele verificării originii și datele de validare	aceeași durată ca înregistrările	în zona protejată (secțiunea 15.4)
Datele contului și lista utilizatorilor autorizați, cu istoricul ei	pe durata contractului și apoi pe durata păstrării înregistrărilor abonatului	necesare pentru dovedirea originii
Jurnalele serviciului	cel puțin 10 ani (secțiunea 6.9)	protejate împotriva modificării

Datele la care se referă amprentele nu sunt primite și nu sunt păstrate de serviciu.

16.2. Verificabilitatea pe termen lung și reînnoirea dovezilor

– registrul rămâne verificabil după expirarea certificatului de sigiliu al serviciului, deoarece punctele de control poartă mărci temporale calificate emise cât timp certificatul era valabil;

– datele de validare ale sigiliului serviciului și ale mărcilor temporale (certificatele și informațiile de revocare) se colectează și se păstrează împreună cu registrul;

– înainte ca o funcție de amprentă, un algoritm de semnătură sau o cheie folosită să devină nesigure conform ECCG ACM ori înainte de expirarea certificatelor pe care se bazează dovezile, CERTDIGITAL emite un punct de control de reînnoire, care acoperă punctele de control anterioare și se sigilează și se marchează temporal cu algoritmi și chei actuale (secțiunea 6.8); înregistrările nu se modifică.

16.3. Schimbarea cheii serviciului

– cheia nouă și certificatul ei se generează înainte de expirarea certificatului în uz sau la schimbarea algoritmilor, în ceremonie (secțiunea 18.2);

– trecerea la cheia nouă se consemnează printr-un punct de control sigilat atât cu cheia veche, cât și cu cheia nouă și marcat temporal calificat (secțiunea 6.8); certificatul nou se publică înainte de prima folosire (secțiunea 10.1);

– după tranziție, cheia veche se distruge sub control dual, cu proces-verbal.

16.4. Exportul pentru abonat

– abonatul poate obține oricând, din cont sau prin interfața de programare, exportul complet al înregistrărilor sale: înregistrările sigilate, semnăturile sau sigiliile utilizatorilor și datele de validare, confirmările, dovezile de includere, punctele de control relevante, certificatele serviciului și specificația formatului;

– exportul permite verificarea independentă a înregistrărilor, fără serviciu (secțiunea 14.3);

– la încetarea contractului, CERTDIGITAL pune exportul la dispoziția abonatului înainte de închiderea contului; înregistrările rămân în registru pe durata de la secțiunea 6.8.

16.5. Predarea registrului la încetarea serviciului

– la încetarea serviciului (secțiunile 6.14 și 18.12), CERTDIGITAL oprește primirea înregistrărilor și emite un punct de control final, sigilat, marcat temporal calificat și publicat;

– registrul complet (înregistrările, punctele de control, dovezile, datele de validare și jurnalele), împreună cu specificația formatului, se predă prestatorului calificat de registre electronice acceptat de ADR, conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530 (REQ-7.12-02A); prestatorul care preia registrul verifică integritatea lui față de punctul de control final și confirmă în scris preluarea;

– fiecare abonat primește exportul complet al înregistrărilor sale (secțiunea 16.4);

– lista punctelor de control, certificatele serviciului și specificațiile rămân publicate, astfel încât registrul să rămână verificabil și după încetare;

– cheia privată a sigiliului serviciului nu se transferă; ea se distruge sub control dual, cu proces-verbal, după emiterea punctului de control final;

– dacă niciun prestator calificat de registre electronice nu preia registrul (Planul de încetare, anexa A11), CERTDIGITAL îl închide printr-o ultimă înregistrare sigilată și marcată temporal, predă fiecărui abonat copia completă a înregistrărilor sale, cu informațiile necesare verificării lor, iar registrul complet, cu punctul de control final, rămâne la custodele înregistrărilor prevăzut în Planul de încetare, pe durata de păstrare stabilită în prezenta declarație; prestatorul care preia registrul se stabilește la data încetării.

17. Controlul accesului și jurnalizarea

17.1. Rolurile și controlul accesului

– rolurile de încredere ale serviciului (administrator de sistem, operator, ofițer de securitate, auditor) sunt separate; aceeași persoană nu cumulează roluri incompatibile (secțiunea 18.4);

– accesul la secvențiator, la componenta de sigilare, la depozitul registrului și la modulele criptografice este permis numai rolurilor de încredere, cu privilegii minime, cu autentificare cu doi factori și numai din rețeaua de administrare;

– operațiile critice (generarea și activarea cheii, schimbarea configurației secvențiatorului, restaurarea, comutarea între centrele de date) se fac sub control dual;

– niciun rol nu are dreptul de a modifica sau de a șterge înregistrări (secțiunea 15.1);

– drepturile de acces se acordă pe bază de cerere aprobată, se revizuiesc periodic și se retrag de îndată la schimbarea atribuțiilor sau la încetarea raportului de muncă.

17.2. Separarea datelor abonaților

– fiecare abonat are acces numai la propriile înregistrări, rapoarte și jurnale ale contului; utilizatorii acționează în limitele drepturilor stabilite de administratorul contului;

– metadatele, semnăturile și certificatele utilizatorilor se păstrează în zona protejată, criptate la stocare, și sunt accesibile numai abonatului și rolurilor de încredere care au nevoie de ele;

– interfața publică de verificare furnizează numai informațiile de la secțiunea 14.2.

17.3. Jurnalizarea

– se jurnalizează evenimentele de la secțiunea 6.9 și, în plus, accesările zonei protejate, modificările listei utilizatorilor autorizați, schimbările de configurație, comutările între centrele de date și operațiile asupra cheilor (ETSI EN 319 401, cl. 7.10);

– fiecare eveniment cuprinde data și ora, sincronizate cu UTC, tipul, rezultatul și identificatorul persoanei sau al componentei care l-a produs;

– jurnalele se transmit în timp real în sistemul centralizat de jurnalizare al CERTDIGITAL, unde sunt protejate împotriva modificării și ștergerii, și se păstrează cel puțin 10 ani (secțiunea 6.9);

– jurnalele nu conțin datele abonaților sau componentele secrete; datele cu caracter personal din jurnale se limitează la cele necesare (identificatori de utilizator, adrese IP), iar accesul la ele este restricționat (RE 2025/2531, REQ-7.9.1-02X);

– jurnalele sunt accesibile auditorilor și ADR; abonatul poate obține extrase privind operațiile din contul său.

17.4. Verificarea continuă a consistenței

– o componentă de monitorizare, separată de secvențiator, verifică fiecare înregistrare nouă (legătura și sigiliul) și fiecare punct de control (sigiliul, marca temporală și legătura cu punctul de control anterior), imediat după emitere;

– periodic, întregul lanț se reverifică de la prima înregistrare sau de la ultimul punct de control de reînnoire, iar copia din centrul de date secundar se compară cu cea din centrul de date principal;

– orice neconcordanță generează o alertă și se tratează conform secțiunii 15.3.

Lanțul se reverifică integral zilnic.

18. Controale operaționale

Se aplică Politicile generale CertDigital și ETSI EN 319 401, cl. 5–7, cu adaptările din Regulamentul de punere în aplicare (UE) 2025/2531 (secțiunile 6.9–6.15). Practicile specifice serviciului sunt descrise mai jos.

18.1. Evaluarea riscurilor

– riscurile serviciului se evaluează înainte de punerea în funcțiune, cel puțin o dată pe an și la orice schimbare semnificativă (ETSI EN 319 401, cl. 5; Regulamentul de punere în aplicare (UE) 2025/2530);

– evaluarea cuprinde și riscurile specifice registrului: apariția a două secvențe paralele, compromiterea cheii serviciului, indisponibilitatea mărcilor temporale calificate, pierderea sincronizării timpului, înscrierea de date cu caracter personal în clar și modificarea neautorizată a registrului de către personal;

– măsurile de tratare se aprobă de conducere, iar riscurile reziduale se acceptă de Directorul General.

18.2. Cheile și modulele criptografice

– cheia privată a sigiliului serviciului se generează în ceremonie, sub control multipersoană, conform procedurii CERTDIGITAL privind generarea cheilor, cu proces-verbal;

– cheia se generează, se păstrează și se folosește numai în modulele criptografice hardware Thales Luna PCIe HSM 7 A790 ale CERTDIGITAL, certificate Common Criteria EAL4+ pe profilul de protecție EN 419 221-5 (NSCIB-CC-2400054-01), ca dispozitiv calificat (eIDAS-2400055-01) și FIPS 140-3 nivel 3; modulele se configurează și se folosesc conform certificării (RE 2025/2531, REQ-7.5-06; secțiunea 6.13);

– cheia nu se poate exporta în clar; copia de rezervă există numai în formă criptată, în al doilea modul, și se gestionează sub control dual;

– cheia se activează de rolurile de încredere, iar componenta de sigilare o folosește numai pentru obiectele de la secțiunea 13.7;

– algoritmul și lungimea cheii sunt cele din profilul certificatului de sigiliu (secțiunea 4.5);

– la sfârșitul utilizării, cheia și copiile ei se distrug sub control dual, cu proces-verbal.

Modulele funcționează cu firmware-ul 7.8.5, versiune acoperită de certificările de mai sus (DPC CERTDIGITAL G5, secțiunea 6.2.1).

18.3. Algoritmii și agilitatea criptografică

– CERTDIGITAL ține evidența algoritmilor folosiți de serviciu (funcția de amprentă a lanțului, algoritmul sigiliului, algoritmii acceptați pentru semnăturile utilizatorilor și pentru TLS) și o

revizuiește cel puțin o dată pe an și la fiecare actualizare a ECCG ACM (RE 2025/2531, REQ-7.5-01X și REQ-7.5-02);

– un algoritm se înlocuiește fără întreruperea serviciului: noul algoritm se introduce printr-un punct de control, identificatorul algoritmului din înregistrări permite verificarea ambelor perioade, iar dovezile anterioare se reînnoiesc (secțiunea 16.2);

– algoritmii pe care ECCG ACM nu îi mai acceptă nu se mai acceptă nici pentru înregistrările noi (secțiunea 13.10).

18.4. Personalul

– rolurile de încredere sunt îndeplinite de angajați ai CENTRUL DE CALCUL S.A., numiți formal, care au cunoștințele, experiența și calificările necesare, dovedite prin instruire formală și atestări, prin experiență practică sau prin combinarea lor (RE 2025/2531, REQ-7.2-04X; secțiunea 6.10);

– personalul cu roluri de încredere primește cel puțin o dată la 12 luni instruire privind amenințările noi și practicile de securitate actuale (REQ-7.2-05X), precum și instruire privind operarea registrului, ceremoniile de chei și răspunsul la incidente; participarea se consemnează;

– verificările la angajare, separarea atribuțiilor și sancțiunile sunt cele din Politicile generale.

18.5. Securitatea fizică

Serviciul funcționează în centrul de date principal și în centrul de date secundar ale CERTDIGITAL (secțiunea 6.11), cu acces fizic controlat și jurnalizat, supraveghere video, sistem de alarmă și alimentare de rezervă, conform Politicilor generale (v2.0). Modulele criptografice și serverele serviciului sunt amplasate în spații la care au acces numai rolurile de încredere; vizitatorii sunt însoțiți și înregistrați.

18.6. Securitatea rețelei

– rețeaua serviciului este împărțită în zone: zona publică (interfața publică de verificare), zona de acces (API și portal) și zona internă (secvențiatorul, depozitul registrului, componenta de sigilare și modulele criptografice); zona internă nu este accesibilă din internet;

– firewall-urile blochează toate protocoalele și accesele care nu sunt necesare funcționării serviciului (RE 2025/2531, REQ-7.8-21X), iar traficul este supravegheat de sisteme de detectare și prevenire a intruziunilor;

– comunicațiile folosesc TLS conform ECCG ACM, cu autentificare reciprocă între componente;

– scanarea de vulnerabilități se efectuează cel puțin o dată pe trimestru (REQ-7.8-13, REQ-7.8-14X), iar testul de penetrare, cel puțin o dată pe an și după schimbările semnificative, de

persoane calificate și independente de echipa de operare (REQ-7.8-17X, REQ-7.8-18X); vulnerabilitățile se remediază în termene stabilite după gravitatea lor.

18.7. Monitorizarea

– disponibilitatea interfețelor, a secvențiatorului, a modulelor criptografice, a serviciului de marcare temporală, a sincronizării timpului și a replicării se monitorizează continuu, cu alertarea personalului de serviciu;

– evenimentele de securitate se corelează în sistemul centralizat de jurnalizare;

– monitorizarea colectează numai datele necesare și ține seama de sensibilitatea lor: nu se colectează datele abonaților, iar accesul la datele de monitorizare este restricționat (RE 2025/2531, REQ-7.9.1-02X; secțiunea 6.9).

18.8. Continuitatea activității

– continuitatea serviciului se asigură conform Procedurii DRP (PO_SI_63) și planului de continuitate a activității, cu centrul de date secundar ca locație de rezervă (secțiunea 6.11);

– registrul se replică în centrul de date secundar; comutarea se face controlat, după confirmarea opririi instanței active, astfel încât secvențiatorul să funcționeze într-o singură instanță (secțiunea 11.2);

– după comutare sau după restaurare, consistența registrului se verifică față de ultimul punct de control publicat, înainte de reluarea primirii înregistrărilor;

– copiile de rezervă se criptează și se păstrează în celălalt centru de date; restaurarea se testează cel puțin o dată pe an;

– disponibilitatea serviciului este de cel puțin 99,5% (secțiunea 6.11).

Înregistrările se replică sincron în centrul de date secundar înaintea transmiterii confirmării, astfel încât nicio înregistrare confirmată să nu se piardă.

18.9. Lanțul de aprovizionare

– furnizorii platformei, ai componentelor software, ai mentenanței modulelor criptografice, ai conectivității și ai altor servicii critice se evaluează înainte de contractare și periodic (ETSI EN 319 401, cl. 7.14);

– contractele cu furnizorii cuprind obligații de securitate, de confidențialitate și de notificare a incidentelor și a vulnerabilităților, precum și dreptul de audit;

– componentele software, inclusiv cele cu sursă deschisă, sunt inventariate și urmărite pentru vulnerabilități; actualizările se testează înainte de instalarea în producție, conform procedurii de gestionare a schimbărilor;

– CERTDIGITAL nu deleagă către terți administrarea registrului, sigilarea sau gestionarea cheilor serviciului (secțiunea 1.3).

18.10. Gestionarea incidentelor

– incidentele se tratează și se notifică conform Procedurii de notificare a incidentelor (00q) și Regulamentului de punere în aplicare (UE) 2025/2530: ADR în cel mult 24 de ore de la luarea la cunoștință, DNSC, ANSPDCP atunci când sunt afectate date cu caracter personal și persoanele afectate (secțiunea 6.11);

– sunt incidente specifice serviciului: neconcordanțele din registru (secțiunea 15.3), suspiciunea de compromitere a cheii serviciului (secțiunea 18.11), pierderea sincronizării timpului, indisponibilitatea prelungită a mărcilor temporale calificate (secțiunea 13.6), accesul neautorizat la zona protejată și înscrierea de date cu caracter personal în clar (secțiunea 15.4);

– abonații ale căror înregistrări sunt afectate sunt informați direct; după fiecare incident se analizează cauzele și se aplică măsuri corective.

18.11. Compromiterea cheii serviciului

– la suspiciunea sau la constatarea compromiterii cheii sigiliului, serviciul oprește sigilarea și primirea înregistrărilor, iar CERTDIGITAL solicită revocarea certificatului de sigiliu și informează ADR, abonații și părțile care se bazează, inclusiv prin publicare pe site (secțiunea 18.10);

– se stabilește momentul compromiterii; înregistrările și punctele de control marcate temporal calificat înainte de acest moment rămân de încredere, deoarece mărcile temporale sunt emise cu cheia distinctă a serviciului de marcare temporală;

– se generează o cheie nouă (secțiunea 18.2), iar primul punct de control sigilat cu ea trimite la ultimul punct de control de încredere; înregistrările sigilate după momentul compromiterii se reverifică și se tratează conform secțiunii 15.3.

18.12. Încetarea serviciului

Încetarea serviciului se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530 (REQ-7.12-02A; secțiunea 6.14): ADR este notificată cu cel puțin trei luni înainte de încetarea planificată (REQ-6.3-04X), abonații sunt informați în termenele din plan, iar registrul se predă conform secțiunii 16.5.

18.13. Evaluarea conformității și notificarea modificărilor

– serviciul este evaluat, cel puțin o dată la 24 de luni, de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162 (EN ISO/IEC 17065 completat de ETSI EN 319 403-1), cu un domeniu care cuprinde serviciul Ledgers/Q

(secțiunea 6.15); ADR este informată cu cel puțin o lună înainte, iar raportul se transmite ADR în cel mult 3 zile lucrătoare;

– atestarea de conformitate se publică în depozitul de documente (secțiunea 10.1);

– CERTDIGITAL efectuează anual un audit intern; neconformitățile se tratează printr-un plan de măsuri corective, urmărit până la închidere;

– orice modificare a prestării serviciului se notifică ADR cu cel puțin o lună înainte de aplicare (REQ-6.3-04X; secțiunea 8.3).

19. Aspecte juridice și comerciale

Tarifele, răspunderea, asigurarea, protecția datelor cu caracter personal, modificările, soluționarea litigiilor, legea aplicabilă și accesibilitatea sunt cele din capitolele 7 și 8 și din termenii și condițiile serviciului (TC-Ledgers). Pe scurt: CERTDIGITAL răspunde conform art. 13 din Regulamentul (UE) nr. 910/2014 (secțiunea 7.4); asigurarea de răspundere civilă profesională a serviciului este cea de la secțiunea 7.5 (Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026); pentru înregistrările abonaților, CERTDIGITAL este persoană împuternicită, iar pentru datele de cont, certificatele utilizatorilor și jurnale, operator, conform Regulamentului (UE) 2016/679 (secțiunea 8.2); verificarea publică este gratuită (secțiunea 8.1); organismul de supraveghere este Autoritatea pentru Digitalizarea României (secțiunea 8.5).

Anexa A – Corespondența practicilor cu Regulamentul de punere în aplicare (UE) 2025/2531 și cu Partea I

Cerință	Conținut	Partea I	Partea a II-a
Regulamentul eIDAS, art. 45l alin. (1) lit. (a)	registru creat și administrat de un prestator calificat	1.3, 4.2, 5.1	11.2, 18.9, 18.13
Regulamentul eIDAS, art. 45l alin. (1) lit. (b)	originea înregistrărilor	4.3, 6.3	12.2, 12.3, 13.3
Regulamentul eIDAS, art. 45l alin. (1) lit. (c)	ordonarea cronologică secvențială unică	4.3, 6.4	13.4–13.6, 13.8
Regulamentul eIDAS, art. 45l alin. (1) lit. (d)	detectarea imediată a modificărilor; integritatea în timp	6.5, 6.8	13.7, 14.4, 15.1, 16.2, 17.4
RE 2025/2531, anexa, pct. 1	definiții: finalitate, legătură criptografică, raport de registru	3.1	11.3, 13.5, 14.5
RE 2025/2531, anexa, pct. 2	rapoarte de registru produse automat	6.6	14.5
REQ-6.1-12, prima liniuță	capacitățile funcționale și tehnice ale platformei registrului	6.1	11, 12.4
REQ-6.1-12, a doua liniuță	mecanismele de autentificare a originii datelor	6.1, 6.3	12.2, 12.3, 13.3
REQ-6.1-12, a treia și a patra liniuță	mecanismele de ordonare cronologică secvențială; legătura criptografică	6.1, 6.4	13.4–13.6, 13.8
REQ-6.1-12, a cincea liniuță	mecanismul de consens și intervalul până la finalitate (nu se aplică registrului centralizat)	4.2, 6.1	11.3
REQ-6.1-12, a șasea liniuță	mecanismele de asigurare a integrității datelor	6.1, 6.5	13.7, 13.8, 14
REQ-6.2-03	termeni și condiții, publici și individuali, înainte de contract	6.2	10.2, 12.1
ETSI EN 319 401, cl. 5	evaluarea riscurilor	6.11	18.1
ETSI EN 319 401, cl. 6.3; REQ-6.3-04X	politica de securitate; notificări ADR (o lună / trei luni)	6.14, 8.3	10.3, 18.12, 18.13
ETSI EN 319 401, cl. 7.1, 7.4	organizarea internă; controlul accesului	6.3	12.3, 17.1, 17.2
REQ-7.2-04X, REQ-7.2-05X	competența personalului; instruire la 12 luni	6.10	18.4
REQ-7.5-01X, REQ-7.5-02	gestionarea criptografiei; agilitate; ECCG ACM	6.12	18.2, 18.3
REQ-7.5-03	originea prin AdES pe certificat calificat (CAdES, XAdES, JAdES cu x5c)	6.3	13.3
REQ-7.5-04	lanț sau arbore de amprente SHA-256 / SHA3-256; mărci temporale calificate	6.4	13.4–13.6, 13.8
REQ-7.5-05 lit. (a)–(c)	integritate prin sigiliu pe certificat calificat; funcții de amprentă	6.5	13.7
REQ-7.5-05 lit. (d)	detectarea imediată a oricărei modificări	6.5	14.3, 14.4, 15.3, 17.4
REQ-7.5-06	cheia prestatorului în dispozitiv certificat (CC / EUCC EAL4+, FIPS 140-3 nivel 3 până la 31.12.2030)	4.5, 6.13	18.2
ETSI EN 319 401, cl. 7.6	securitatea fizică	6.11	18.5
ETSI EN 319 401, cl. 7.7	securitatea operațiunilor	6.11	18.7–18.9
REQ-7.8-13, 7.8-14X, 7.8-17X, 7.8-18X, 7.8-21X	scanare trimestrială; test de penetrare anual; firewall	6.13	18.6
REQ-7.9.1-02X	monitorizarea ține seama de sensibilitatea informațiilor	6.9	17.3, 18.7
ETSI EN 319 401, cl. 7.9	gestionarea incidentelor	6.11	15.3, 18.10, 18.11

Cerință	**Conținut**	**Partea I**	**Partea a II-a**
ETSI EN 319 401, cl. 7.10	jurnalizarea evenimentelor	6.9	17.3
ETSI EN 319 401, cl. 7.11	continuitatea activității	6.11	18.8
REQ-7.12-02A	plan de încetare conform 2025/2530; predarea registrului	6.14	16.5, 18.12
ETSI EN 319 401, cl. 7.13	conformitatea; evaluarea conformității	6.15	18.13
ETSI EN 319 401, cl. 7.14	lanțul de aprovizionare	1.3	18.9
RE 2025/2531, anexa, pct. 3 lit. (b)	ISO 23257 / ISO/TS 23635 — numai pentru DLT; nu se aplică	2.1, 4.2	11.2, 11.3
Regulamentul (UE) 2016/679; Ghidul EDPB 02/2025	fără date personale în clar; amprente cu componentă secretă	4.4, 8.2	13.1, 14.2, 15.4, 17.2