

Politica și declarația de practici a serviciului calificat de arhivare electronică

CertDigital QEArch

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 arhivare electronică; Reg. (UE) 2025/2532 și CEN/TS 18170; 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
1.4	Ofițer de Securitate IT	Punctul de acces al serviciului calificat: https://arhivare.certdigital.ro (secțiunile 4.2 și 11.4)	27.10.2026
1.5	Ofițer de Securitate IT	Infrastructura (14.1): platforma sistemului AE se descrie generic, fără produsele folosite; securitatea fizică (20.4): accesul se descrie ca autentificare în mai mulți factori, fără enumerarea factorilor, care rămân în documentația internă de securitate; conținutul neschimbat în rest	03.11.2026
1.6	Ofițer de Securitate IT	Corespondența cu ISO 14721:2025, în anexa B (nouă): comunitatea desemnată, regula legăturilor, limba documentului, informațiile de reprezentare, păstrarea fișierului primit,	12.11.2026

		colecțiile și structura exportului (3, 5.2, 6, 10–13, 16); semnarea la distanță, PAdES și JAdES, și marca temporală prin QPS (11.4, 13); aplicația sistemului AE, avizul ADR și obligațiile față de ADR (4.2, 6.15, 20.8); replicarea sistemului AE la 5 minute, copiile criptate, copia offline și testul de restaurare la 6 luni (6.13, 14, 20.7); eliminarea la cererea titularului (18); încetarea: notificarea cu 60 de zile înainte și succesorul (20.10)	
1.7	Ofițer de Securitate IT	Verificarea pe textul complet CEN/TS 18170:2025: acordurile de serviciu și de depunere, pachetele de informații E-ARK (SIP, AIP, DIP), formatele și conversia, verificările la primire, integritatea și exhaustivitatea, a treia locație pentru AIP (București), jurnalul de audit (evenimentele critice, PREMIS), rapoartele serviciului, eliminarea, exportul și transferul, încrederea în semnăturile și sigiliile calificate și în profilul general (art. 1 din Regulamentul (UE) 2025/2532)	16.11.2026

Cuprins

PARTEA I – Politica serviciului 10
1. Introducere 10
1.1. Prezentare generală 10
1.2. Identificarea documentului și a politicii 10
1.3. Participanții 11
1.4. Utilizarea serviciului 11
1.5. Administrarea documentului 12
2. Referințe normative 13
2.1. Acte normative și standarde 13
3. Definiții și acronime 14
3.1. Definiții 14
3.2. Acronime 14
4. Concepte generale 16
4.1. Serviciul și componentele sale 16
4.2. Platforma serviciului 16
4.3. Profilurile de arhivare 17
4.4. Relația cu serviciul de păstrare calificată 17
4.5. Relația cu regimul național al arhivării electronice 17
4.6. Identitatea serviciului și sigiliul serviciului 18
5. Politica serviciului 19
5.1. Identificare și conformitate 19
5.2. Comunitatea utilizatorilor și aplicabilitatea 19
5.3. Modificarea politicii 19
6. Cerințele privind practicile 20
6.1. Publicare și depozit 20
6.2. Termeni și condiții; acordurile cu abonatul 20
6.3. Depunerea și stabilirea originii 20
6.4. Raportul de confirmare a arhivării 21
6.5. Păstrarea, integritatea și confidențialitatea 21
6.6. Documentele care conțin semnături sau sigilii calificate 22

6.7. Lizibilitatea și migrarea formatelor 22
6.8. Regăsirea, accesul și livrarea 23
6.9. Raportul de integritate la extragere 23
6.10. Perioada de păstrare și eliminarea 23
6.11. Timpul de încredere și jurnalele 24
6.12. Personalul 24
6.13. Controale privind facilitățile, managementul și operarea 24
6.14. Controale criptografice și de rețea 25
6.15. Notificări către ADR și încetarea serviciului 26
6.16. Evaluarea conformității 26
7. Obligații și răspundere 27
7.1. Obligațiile CERTDIGITAL 27
7.2. Obligațiile abonatului 27
7.3. Obligațiile părților care se bazează 27
7.4. Răspunderea 27
7.5. Asigurarea 28
8. Alte aspecte comerciale și juridice 29
8.1. Tarife 29
8.2. Protecția datelor cu caracter personal 29
8.3. Modificări 29
8.4. Soluționarea litigiilor 29
8.5. Legea aplicabilă și cadrul legal 30
8.6. Alte prevederi 30
9. Corespondența cu cerințele Regulamentului (UE) 2025/2532 și ale CEN/TS 18170 31
9.1. Tabel de corespondență 31
PARTEA A II-A – Declarația de practici 33
10. Publicare și depozit 33
10.1. Documentele publicate 33
10.2. Disponibilitatea depozitului și versiunile 34
11. Accesul la serviciu 35
11.1. Contractarea serviciului 35
11.2. Spațiul abonatului și rolurile utilizatorilor 35
11.3. Autentificarea 35

11.4. Interfața web 36
11.5. Interfața de programare 36
11.6. Limitele de utilizare 36
12. Depunerea și acceptarea documentelor 37
12.1. Etapele depunerii 37
12.2. Pachetul depus și metadatele obligatorii 37
12.3. Stabilirea originii 38
12.4. Verificările la primire 38
12.5. Formatele admise și regulile de conversie 39
12.6. Confirmarea de primire și codurile de răspuns 41
12.7. Raportul de confirmare a arhivării 42
13. Integritatea și dovezile de arhivare 43
13.1. Amprentele criptografice 43
13.2. Semnătura titularului dreptului de dispoziție 43
13.3. Sigiliul calificat al serviciului 43
13.4. Mărcile temporale calificate și timpul de referință 44
13.5. Pachetul arhivat (AIP) și dovezile de arhivare 44
13.6. Reînnoirea dovezilor 46
13.7. Verificarea periodică a integrității 46
14. Stocarea, replicarea și copiile de rezervă 48
14.1. Infrastructura și localizarea datelor 48
14.2. Replicarea între centrele de date 48
14.3. Copiile de rezervă și restaurarea 49
14.4. Criptarea la stocare și confidențialitatea 50
15. Menținerea validității semnăturilor și sigiliilor calificate (profilul 1.3.6.1.4.1.47898.12.1.2) 51
15.1. Admiterea documentelor în profil 51
15.2. Utilizarea serviciului de păstrare calificată 51
15.3. Monitorizarea și evenimentele de păstrare 51
15.4. Documentele semnate din profilul general 52
16. Regăsirea, livrarea și dovada integrității 53
16.1. Căutarea 53
16.2. Livrarea documentelor și copiile 53
16.3. Raportul de integritate 53

16.4. Exportul complet și restituirea arhivei 54
16.5. Verificarea de către părțile care se bazează 55
17. Controlul accesului și jurnalizarea 56
17.1. Modelul de autorizare 56
17.2. Gestionarea conturilor 56
17.3. Accesul personalului CERTDIGITAL 56
17.4. Evenimentele jurnalizate 57
17.5. Protecția și păstrarea jurnalelor 57
18. Perioadele de păstrare și eliminarea 59
18.1. Stabilirea și modificarea perioadei de păstrare 59
18.2. Notificările înainte de expirare 59
18.3. Blocarea legală 60
18.4. Aprobarea și executarea eliminării 60
18.5. Raportul de eliminare 60
19. Lizibilitatea și migrarea 62
19.1. Monitorizarea formatelor 62
19.2. Migrarea formatelor 62
19.3. Migrarea suporturilor și a platformei 62
20. Controale operaționale 64
20.1. Cheile serviciului și modulele criptografice 64
20.2. Algoritmii criptografici 64
20.3. Personalul și rolurile de încredere 64
20.4. Securitatea fizică 65
20.5. Securitatea rețelei și gestionarea vulnerabilităților 65
20.6. Monitorizarea și disponibilitatea 65
20.7. Continuitatea și recuperarea în caz de dezastru 66
20.8. Lanțul de aprovizionare 67
20.9. Gestionarea incidentelor 67
20.10. Încetarea serviciului și transferul arhivelor 67
20.11. Evaluarea conformității și auditul 68
21. Aspecte juridice și comerciale 70
Anexa A – Corespondența practicilor cu cerințele Regulamentului (UE) 2025/2532 și ale CEN/TS 18170 71
Anexa B – Corespondența cu modelul de referință OAIS (ISO 14721:2025) 73

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 arhivare electronică** (art. 3 pct. 48 și 49, art. 45i și 45j din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183) și descrie practicile prin care le îndeplinește.

Serviciul asigură primirea, stocarea, regăsirea și ștergerea datelor electronice și a documentelor electronice încredințate de abonați, pentru a le asigura durabilitatea și lizibilitatea și pentru a le păstra integritatea, confidențialitatea și dovada originii pe toată perioada de păstrare legală sau contractuală. Datele și documentele păstrate prin serviciu beneficiază de prezumția de integritate și de acuratețe a originii pe toată durata păstrării de către CERTDIGITAL (art. 45i alin. (2)). În terminologia CEN/TS 18170, serviciul este un serviciu de încredere de arhivare electronică (EATS), iar CERTDIGITAL este prestatorul acestuia (EATSP).

Partea I (politica serviciului, capitolele 1–9) stabilește **ce** garantează CERTDIGITAL. **Cum** sunt îndeplinite cerințele este descris în Partea a II-a (declarația de practici, capitolele 10–21). Pentru păstrarea calificată a semnăturilor și sigiliilor electronice calificate se aplică Politica și declarația de practici a serviciului de păstrare calificată (PSPPS), pentru mărcile temporale calificate Politica și declarația de practici a serviciului calificat de marcare temporală (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 arhivare electronică CertDigital (PDP-QEArch)
Titlu în limba engleză	CertDigital Qualified Electronic Archiving Service Policy and Practice Statement
Versiune	1.7
Data	16.11.2026
Identificatorul documentului (OID)	1.3.6.1.4.1.47898.12.1
Profilul de arhivare general	1.3.6.1.4.1.47898.12.1.1 (date și documente electronice, indiferent dacă sunt semnate sau sigilate)
Profilul de arhivare cu păstrare calificată	1.3.6.1.4.1.47898.12.1.2 (documente care conțin semnături sau sigilii electronice calificate, a căror încredere se menține prin serviciul de păstrare calificată CERTDIGITAL, secțiunea 4.4)

Element	Valoare
Declarația de practici	declarația de practici este inclusă în prezentul document (Partea a II-a); identificatorul 1.3.6.1.4.1.47898.12.2 nu se mai folosește
Specificații de referință	CEN/TS 18170:2025, cu adaptările din anexa la Regulamentul de punere în aplicare (UE) 2025/2532
Tipul de serviciu (ETSI TS 119 612)	`http://uri.etsi.org/TrstSvc/Svctype/ElectronicArchiving/Q`
Identitatea serviciului în Lista de încredere (după înscriere)	certificatul calificat de sigiliu al serviciului (secțiunea 4.6)
Generație	serviciul se prestează în generația G5 a infrastructurii CERTDIGITAL
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-qearch_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Identificatorii sunt înscriși în CERTDIGITAL_OID_MAP. Certificatul de sigiliu al serviciului conține identificatorul prezentului document (1.3.6.1.4.1.47898.12.1); identificatorii profilurilor se înscriu în rapoartele de confirmare și în dovezile de arhivare.

1.3. Participanții

– **prestatorul (EATSP)**: CERTDIGITAL, care răspunde în ansamblu de serviciu, inclusiv atunci când folosește serviciile calificate proprii de păstrare și de marcare temporală;

– **abonatul (depunătorul)**: persoana fizică sau juridică ce încheie contractul cu CERTDIGITAL și depune datele și documentele în arhivă;

– **titularul dreptului de dispoziție**: persoana desemnată de abonat să decidă asupra documentelor arhivate (depunere, acces, termen de păstrare, eliminare); poate fi abonatul însuși;

– **utilizatorii autorizați**: persoanele cărora abonatul sau titularul dreptului de dispoziție le acordă acces la documentele arhivate;

– **beneficiarii autorizați și părțile care se bazează**: persoanele care primesc documente extrase din arhivă împreună cu raportul de integritate (secțiunea 6.9) și se bazează pe acesta.

CERTDIGITAL nu deleagă către terți operarea serviciului, păstrarea arhivei sau gestionarea cheilor serviciului.

1.4. Utilizarea serviciului

Serviciul se utilizează pentru păstrarea pe termen lung, cu valoare probatorie, a datelor și documentelor electronice ale abonaților, pe perioada de păstrare legală sau contractuală stabilită de aceștia. Serviciul nu modifică conținutul documentelor, cu excepția schimbărilor de suport sau de format electronic făcute conform prezentei politici (art. 45j alin. (1) lit. (c)). Serviciul nu înlocuiește

obligațiile legale ale abonatului privind arhivarea (de exemplu cele din Legea Arhivelor Naționale nr. 16/1996), ci îl ajută să le îndeplinească.

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. 48 și 49, art. 13, 19a, 20, 21, 24, 45i și 45j;

– Regulamentul de punere în aplicare (UE) 2025/2532 (standardele de referință și specificațiile pentru serviciile calificate de arhivare electronică);

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

– Regulamentul de punere în aplicare (UE) 2025/1946 (păstrarea calificată a semnăturilor și sigiliilor electronice calificate) și Regulamentul de punere în aplicare (UE) 2025/1945 (validarea semnăturilor și sigiliilor electronice);

– Regulamentul de punere în aplicare (UE) 2025/1929 (marcarea temporală calificată); Regulamentul de punere în aplicare (UE) 2025/2162 (acreditarea organismelor de evaluare a conformității);

– CEN/TS 18170:2025 (cerințe funcționale pentru serviciile de arhivare electronică);

– ETSI EN 319 401 V3.1.1 (cerințe generale pentru prestatorii de servicii de încredere); ETSI EN 319 421 V1.3.1 (mărci temporale);

– ISO 14721:2025 (modelul de referință OAIS);

– ETSI EN 319 122-1, EN 319 132-1, EN 319 142-1 și EN 319 162-1 (formatele CAdES, XAdES, PAdES și ASiC), conform Regulamentului de punere în aplicare (UE) 2026/248, și ETSI TS 119 182-1 (JAdES); ETSI TS 119 512 (protocoalele serviciilor de păstrare); ISO 19005 (PDF/A);

– documentul „Agreed Cryptographic Mechanisms” al ECCG, publicat de ENISA; Regulamentele de punere în aplicare (UE) 2024/482 și 2024/3144 (schema EUCC); ISO/IEC 15408:2022, părțile 1–5 (Common Criteria), și FIPS PUB 140-3 (2019), pentru modulele criptografice (secțiunea 6.14);

– Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026; Legea nr. 135/2007 privind arhivarea documentelor în formă electronică, republicată, și Ordinul MCID nr. 20.717/2024; Legea Arhivelor Naționale nr. 16/1996, republicată; Regulamentul (UE) 2016/679 și Legea nr. 190/2018.

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

3. Definiții și acronime

3.1. Definiții

– **arhivare electronică** — serviciul care asigură primirea, stocarea, recuperarea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a păstra integritatea, confidențialitatea și dovada originii acestora pe parcursul întregii perioade de păstrare (art. 3 pct. 48 din Regulamentul eIDAS);

– **perioadă de păstrare** — perioada, legală sau contractuală, stabilită de abonat pentru fiecare document sau tip de document, în care CERTDIGITAL păstrează documentul;

– **profil de arhivare** — ansamblul regulilor aplicate unei categorii de documente (formate admise, verificări la depunere, dovezi, păstrare, eliminare), identificat printr-un OID;

– **pachet de informații** — unitatea de informații din modelul OAIS: pachetul depus (SIP), pachetul arhivat (AIP) și pachetul livrat (DIP) (ISO 14721:2025, 2.3.4 și 4.3.3); „pachetul" din structura arhivei unui abonat în sistemul AE (compartiment, pachet, dosar) este o unitate de clasificare a documentelor, nu un pachet de informații;

– **manifestul pachetului arhivat** — lista amprentelor criptografice ale obiectelor și ale metadatelor unui AIP, sigilată cu sigiliul calificat al serviciului și marcată temporal calificat, care constituie dovada de arhivare a pachetului (secțiunea 13.5);

– **raport de confirmare a arhivării** — documentul emis la depunere prin care CERTDIGITAL confirmă primirea și arhivarea, cu identificatorii, amprentele și data depunerii;

– **raport de integritate** — raportul furnizat automat la extragerea unui document, care confirmă că documentul beneficiază de prezumția de integritate de la începutul perioadei de păstrare până în momentul extragerii (art. 45j alin. (1) lit. (d));

– **raport de eliminare** — raportul emis la eliminarea documentelor, prin care CERTDIGITAL confirmă ștergerea lor din toate copiile (secțiunile 6.10 și 18.5);

– **eliminare** — ștergerea definitivă a unui document arhivat și a tuturor copiilor sale, la expirarea perioadei de păstrare, la încetarea contractului, după termenul de export (secțiunea 16.4), sau, înainte de expirarea perioadei, la cererea titularului dreptului de dispoziție, cu respectarea termenelor legale de păstrare și numai prin fluxul de eliminare de la capitolul 18.

3.2. Acronime

Acronim	Semnificație
AdES	semnătură sau sigiliu electronic avansat în formatele standardizate de ETSI (CAdES, XAdES, PAdES, JAdES), inclusiv în containere ASiC
AIC	colecție de informații arhivate (Archival Information Collection)
AIP	pachet de informații arhivat (Archival Information Package)
AIU	unitate de informații arhivate (Archival Information Unit)
API	interfață de programare a aplicațiilor (Application Programming Interface)

Acronim	**Semnificație**
DIP	pachet de informații livrat (Dissemination Information Package)
EATS / EATSP	serviciu de încredere de arhivare electronică / prestatorul acestuia (CEN/TS 18170)
ECCG ACM	documentul „Agreed Cryptographic Mechanisms” al Grupului european de certificare a securității cibernetice
HSM	modul criptografic hardware (Hardware Security Module)
OAIS	modelul de referință pentru un sistem deschis de informații arhivistice (ISO 14721)
PDI	informații de descriere pentru păstrare (Preservation Description Information)
QEArch	serviciul calificat de arhivare electronică
QPS	serviciul calificat de păstrare a semnăturilor și sigiliilor electronice calificate CERTDIGITAL
QTST	marcă temporală electronică calificată
RPO	pierderea maximă acceptată de date, exprimată în timp (Recovery Point Objective)
RTO	durata maximă de restabilire a serviciului (Recovery Time Objective)
SIP	pachet de informații depus (Submission Information Package)

4. Concepte generale

4.1. Serviciul și componentele sale

Serviciul urmează modelul de referință OAIS (ISO 14721:2025; corespondența termenilor și a componentelor lui cu prezentul document este în anexa B) și structura pachetelor de informații din CEN/TS 18170, cl. 8–11, și cuprinde:

– **depunerea**: primirea pachetelor SIP, verificarea lor și stabilirea originii (secțiunea 6.3);

– **arhivarea**: transformarea în pachete AIP, cu metadatele și dovezile de arhivare, și emiterea raportului de confirmare (secțiunile 6.4 și 6.5);

– **păstrarea**: stocarea protejată, verificarea periodică a integrității, menținerea dovezilor, a lizibilității și a încrederii în semnăturile și sigiliile calificate (secțiunile 6.5–6.7);

– **regăsirea și livrarea**: căutarea, accesul controlat și livrarea pachetelor DIP împreună cu raportul de integritate (secțiunile 6.8 și 6.9);

– **eliminarea**: ștergerea la expirarea perioadei de păstrare, cu dovadă (secțiunea 6.10).

Provocările arhivării pe termen lung, indiferent de suport și pe tot ciclul de viață al documentelor, de la depunere până la eliminare, pe care serviciul le tratează sunt (CEN/TS 18170, cl. 6.1 lit. a)): învechirea formatelor și a programelor de redare (secțiunile 6.7 și 19.1–19.2); învechirea suporturilor de stocare și a platformei (secțiunea 19.3); slăbirea algoritmilor criptografici și expirarea certificatelor pe care se bazează dovezile (secțiunile 6.5, 6.14 și 13.6); pierderea sau alterarea datelor (secțiunile 6.5, 13.7 și capitolul 14); accesul neautorizat și păstrarea confidențialității (secțiunea 6.5 și capitolul 17); menținerea înțelegerii documentelor de către comunitatea desemnată (secțiunea 5.2); modificarea cadrului legal și a termenelor de păstrare (secțiunea 10.2 și capitolul 18); continuitatea custodiei la încetarea contractului sau a serviciului (secțiunile 16.4 și 20.10).

4.2. Platforma serviciului

Serviciul este prestat prin sistemul electronic de arhivare **CertDigital eArhivare – Arhivare Electronică (AE)**, dezvoltat de CENTRUL DE CALCUL S.A. Pentru sistemul AE, Autoritatea pentru Digitalizarea României a emis avizul tehnic nr. 34/14.07.2025, pe baza documentației sistemului din 2025; dezvoltările și modificările ulterioare ale sistemului se notifică ADR conform secțiunii 6.15. Sistemul este găzduit în centrul de date propriu din Târgu Jiu, autorizat de ADR (Decizia nr. 402/13.07.2026), și în centrul de date secundar, cu replicarea datelor între cele două locații (secțiunea 6.13). Cheile serviciului se păstrează în module criptografice certificate (secțiunea 6.14).

Punctul de acces al serviciului calificat este https://arhivare.certdigital.ro. Adresa https://cde.certdigital.ro/ae/ aparține versiunii din 2025 a sistemului AE și nu este punct de acces al serviciului calificat.

4.3. Profilurile de arhivare

Profil	Conținut	Menținerea integrității și a originii
General (47898.12.1.1)	date și documente electronice în formatele admise (secțiunea 6.7), cu metadatele de la depunere	amprente criptografice ale fiecărui obiect, sigiliul calificat al serviciului și mărci temporale calificate pe dovezile de arhivare, reînnoite înainte de slăbirea algoritmilor sau de expirarea certificatelor
Cu păstrare calificată (47898.12.1.2)	documente care conțin semnături sau sigilii electronice calificate (PAdES, XAdES, CAdES și containere ASiC)	în plus, încrederea în semnăturile și sigiliile calificate se menține dincolo de perioada lor de valabilitate tehnologică prin serviciul de păstrare calificată CERTDIGITAL (secțiunea 4.4)

Profilul aplicat fiecărui document se stabilește la depunere și se înscrie în raportul de confirmare. Pentru fiecare profil, structura AIP, funcțiile și sintaxa componentelor lui sunt descrise în secțiunea 13.5 și în specificația pachetelor de informații (secțiunea 12.2; CEN/TS 18170, cl. 10.1), iar formatele admise și formatele-țintă de conversie sunt cele din secțiunea 12.5 (CEN/TS 18170, cl. 10.5.2).

4.4. Relația cu serviciul de păstrare calificată

Pentru documentele care conțin semnături sau sigilii electronice calificate, CERTDIGITAL menține încrederea în acestea, inclusiv dincolo de perioada lor de valabilitate tehnologică, precum și integritatea și acuratețea originii lor, cel puțin până la sfârșitul perioadei de păstrare (art. 1 alin. (1) din Regulamentul de punere în aplicare (UE) 2025/2532). În acest scop, CERTDIGITAL folosește propriul serviciu de păstrare a semnăturilor și sigiliilor electronice calificate, cu obiectivele de păstrare a semnăturilor digitale, a datelor generale și de augmentare, conform PSPPS. Pentru acest serviciu se solicită statutul calificat, în aceeași evaluare a conformității ca serviciul de arhivare (secțiunea 20.8); după înscrierea lui în Lista de încredere a României, CERTDIGITAL se bazează pe el în sensul art. 1 alin. (2), iar până atunci asigură direct îndeplinirea cerințelor art. 1 alin. (1), prin practicile din capitolul 15.

4.5. Relația cu regimul național al arhivării electronice

CERTDIGITAL prestează serviciul și în calitate de administrator de arhivă electronică, potrivit Legii nr. 135/2007 și Ordinului MCID nr. 20.717/2024, prin sistemul AE avizat (secțiunea 4.2). Prezentul document reprezintă și politica de conservare a documentelor pe termen lung cerută de aceste reglementări.

4.6. Identitatea serviciului și sigiliul serviciului

Rapoartele de confirmare, rapoartele de integritate, dovezile de arhivare și rapoartele de eliminare poartă **sigiliul electronic calificat al serviciului**, creat cu un certificat calificat de sigiliu emis pentru CENTRUL DE CALCUL S.A. și dedicat serviciului. Același certificat va identifica serviciul în Lista de încredere a României, după înscriere. Fiecare sigiliu este însoțit de o marcă temporală calificată.

Certificatul serviciului este CERTDIGITAL QEARCH 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 20.1). Profilul lui este descris în DPC CERTDIGITAL G5, secțiunea 7.1.2, iar certificatul se publică la http://certs.certdigital.ro/certdigital_qearch_g5.crt. Certificatul CERTDIGITAL QEARCH Service G4 nu se folosește pentru acest serviciu (IER-PKI, secțiunea 3.3).

5. Politica serviciului

5.1. Identificare și conformitate

CERTDIGITAL declară conformitatea serviciului cu CEN/TS 18170:2025, cu adaptările din anexa la Regulamentul de punere în aplicare (UE) 2025/2532, ceea ce atrage prezumția de conformitate cu cerințele art. 45j alin. (1) din Regulamentul eIDAS (art. 45j alin. (2)). Conformitatea este evaluată de un organism de evaluare a conformității acreditat (secțiunea 6.16). 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 fizice și juridice, autorităților și instituțiilor publice care trebuie sau doresc să păstreze pe termen lung documente electronice cu valoare probatorie, precum și părților care se bazează pe documentele extrase din arhivă.

Comunitatea desemnată a serviciului (ISO 14721:2025, 1.6.2 și 3.2) cuprinde abonații, titularii dreptului de dispoziție, utilizatorii și beneficiarii autorizați și părțile care se bazează pe documentele extrase, inclusiv autoritățile, instanțele și arhivele cărora documentele le sunt prezentate sau predate. Baza ei de cunoștințe presupune: cunoașterea limbii documentului, indicată la depunere (secțiunea 12.2); folosirea programelor larg disponibile pentru formatele din lista formatelor admise (secțiunea 12.5); folosirea unui validator de semnături și sigilii electronice conform Regulamentului de punere în aplicare (UE) 2025/1945, pentru verificarea rapoartelor și a dovezilor (secțiunea 16.5); pentru documentele fiecărui abonat, accesul la nomenclatorul arhivistic și la schema de metadate a tipului de document, care se păstrează împreună cu documentele. Informațiile de reprezentare păstrate în fiecare AIP (secțiunea 13.5) sunt stabilite pentru această bază de cunoștințe; comunitatea desemnată și baza ei de cunoștințe se reevaluează la revizia anuală a prezentului document și la verificarea anuală a formatelor (secțiunile 10.2 și 19.1). Corespondența cu modelul OAIS este în anexa B.

5.3. Modificarea politicii

Dacă o modificare a prezentei politici sau a unui profil afectează garanțiile oferite pentru documentele deja arhivate, identificatorul politicii sau al profilului se schimbă. Documentele arhivate rămân guvernate de profilul înscris în raportul de confirmare, până la migrarea lor, cu acordul abonatului, într-un profil nou.

6. Cerințele privind practicile

6.1. Publicare și depozit

Prezentul document, termenii și condițiile serviciului (TC-QEArch), profilurile de arhivare, lista formatelor admise, lista codurilor de răspuns la depunere și certificatul de sigiliu al serviciului sunt publicate la https://www.certdigital.ro/repository/, 24/7, public și fără restricții de acces (secțiunea 10.1). Partea a II-a descrie, pentru fiecare profil, formatele admise (secțiunea 12.5), metadatele obligatorii (secțiunea 12.2), verificările la depunere (secțiunea 12.4), dovezile emise (capitolul 13), algoritmii folosiți (secțiunea 20.2) și termenele aplicabile (capitolul 18), conform CEN/TS 18170, cl. 6.1, și ETSI EN 319 401, cl. 5 și 6.1.

6.2. Termeni și condiții; acordurile cu abonatul

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: profilurile, formatele admise, perioadele de păstrare, accesul, eliminarea, restituirea la încetare, tarifele, răspunderea și limitările ei (CEN/TS 18170, cl. 6.2; Regulamentul (UE) 2025/2532, anexa, lit. (c)).

Contractul cu abonatul cuprinde (CEN/TS 18170, cl. 6.4):

– **acordul de serviciu**: profilurile, nivelul serviciului, perioadele de păstrare, accesul, raportarea, restituirea și transferul arhivei;

– **acordul de depunere**: formatele și metadatele pachetelor depuse, modul de transmitere, verificările făcute la primire, codurile de răspuns și tratarea legăturilor din documente către resurse externe (ISO 14721:2025, 2.6.3).

6.3. Depunerea și stabilirea originii

Depunerea respectă acordul de depunere și CEN/TS 18170, cl. 9 (pachetul SIP, formatele obiectelor, transmiterea, primirea și verificarea depunerii):

– abonatul și utilizatorii săi se autentifică în serviciu prin mijloace de autentificare puternică, cu cel puțin doi factori, sau cu certificat calificat;

– originea datelor depuse se stabilește de CERTDIGITAL; atunci când originea se stabilește prin semnătura sau sigiliul depunătorului ori al titularului dreptului de dispoziție, semnătura sau sigiliul trebuie să fie **calificate** (Regulamentul (UE) 2025/2532, anexa, lit. (e));

– semnăturile și sigiliile din documentele depuse se validează la depunere conform Regulamentului de punere în aplicare (UE) 2025/1945, iar rezultatul validării (inclusiv rezultatele nedeterminate, marcate explicit) se păstrează în AIP; validarea nu condiționează arhivarea în profilul general, dar numai documentele cu semnături sau sigilii calificate valide se arhivează în profilul cu păstrare calificată;

– se verifică formatul fiecărui obiect, completitudinea metadatelor obligatorii, integritatea transferului (amprentă calculată de depunător și recalculată la primire) și absența codului malițios;

– fiecare depunere conține cel puțin: depunătorul, emitentul și titularul dreptului de dispoziție, tipul și data documentului, nivelul de clasificare și regimul de acces, formatul, limba documentului, cuvintele-cheie și perioada de păstrare; pentru arhivele supuse Legii nr. 135/2007 și Legii nr. 16/1996, metadatele includ și încadrarea în nomenclatorul arhivistic al abonatului;

– la primire, CERTDIGITAL transmite automat depunătorului o confirmare de primire, cu un cod de răspuns din lista publicată (secțiunea 12.6); pachetele care nu trec verificările se resping, cu codul și motivarea respingerii; respingerea se jurnalizează.

6.4. Raportul de confirmare a arhivării

Pentru fiecare depunere acceptată, CERTDIGITAL emite automat un raport de confirmare a arhivării (CEN/TS 18170, cl. 14), cu sigiliul calificat al serviciului și cu marcă temporală calificată, care conține: identificatorul unic persistent al fiecărui obiect, amprentele criptografice ale acestora, profilul de arhivare, perioada de păstrare, rezultatul verificărilor de la depunere și data și ora arhivării. Raportul se transmite depunătorului și se păstrează în AIP.

6.5. Păstrarea, integritatea și confidențialitatea

– fiecare AIP conține obiectele depuse, exact cum au fost primite, metadatele descriptive și de păstrare, informațiile de reprezentare (formatul și, după caz, schema, descrierea câmpurilor și limba documentului), raportul de confirmare și dovezile de arhivare (CEN/TS 18170, cl. 10.2; ISO 14721:2025, 4.3.2);

– infrastructura de stocare și localizarea ei sunt descrise în secțiunea 14.1; datele arhivate nu părăsesc Uniunea Europeană (CEN/TS 18170, cl. 10.3);

– documentele sunt protejate împotriva pierderii și modificării, cu excepția schimbărilor de suport sau de format făcute conform secțiunii 6.7 (art. 45j alin. (1) lit. (c); CEN/TS 18170, cl. 10.4);

– arhiva se păstrează în cel puțin două copii, în centrele de date ale CERTDIGITAL din România, situate în locații diferite, iar pentru ca AIP-urile să se afle permanent în locații îndepărtate geografic, și în locația CERTDIGITAL din București (secțiunea 14.1; CEN/TS 18170, cl. 10.4); integritatea fiecărei copii se verifică cel puțin anual, prin recalcularea amprentelor, și la fiecare acces; orice neconcordanță se tratează ca incident și se corectează din copia validă;

– dovezile de arhivare (amprente, sigilii, mărci temporale) se reînnoiesc înainte ca algoritmii folosiți să devină nesiguri, conform ECCG ACM, sau înainte de expirarea certificatelor pe care se bazează;

– confidențialitatea datelor se asigură pe tot ciclul de viață al arhivei, de la depunere până la eliminare: comunicații criptate (TLS 1.2 sau superior), criptarea datelor arhivate la stocare și control strict al accesului (Regulamentul (UE) 2025/2532, anexa, lit. (e)); criptarea la stocare folosește AES-256, cu chei separate pentru fiecare abonat, gestionate în modulul criptografic (secțiunea 14.4).

6.6. Documentele care conțin semnături sau sigilii calificate

Pentru profilul cu păstrare calificată (47898.12.1.2), dovezile de validare ale semnăturilor și sigiliilor calificate (lanțul de certificate, informațiile privind starea certificatelor, mărcile temporale) se colectează și se păstrează în AIP, iar încrederea în semnături și sigilii se menține prin serviciul de păstrare calificată CERTDIGITAL, cu augmentarea periodică a dovezilor, până la sfârșitul perioadei de păstrare (secțiunea 4.4).

6.7. Lizibilitatea și migrarea formatelor

Se aplică CEN/TS 18170, cl. 9.5, 10.2.5, 10.2.6 și 10.5:

– CERTDIGITAL publică lista formatelor (secțiunea 12.5) pentru care garantează lizibilitatea pe toată perioada de păstrare (de exemplu PDF/A, XML cu schema asociată, formatele de semnătură AdES și ASiC, formate de imagine și text deschise);

– documentele în alte formate se pot arhiva numai dacă formatele lor sunt enumerate în acordul de depunere, cu acordul abonatului, și numai cu garantarea integrității, nu și a lizibilității; mențiunea se înscrie în raportul de confirmare; documentele în formate care nu sunt admise și nici enumerate în acordul de depunere se resping (CEN/TS 18170, cl. 9.5);

– CERTDIGITAL monitorizează viabilitatea formatelor admise; dacă un format devine depășit, documentele se migrează într-un format admis, cu păstrarea originalului și a legăturii dintre original și copia migrată, iar migrarea se documentează într-o dovadă sigilată și marcată temporal;

– migrarea nu modifică dovada integrității documentului original; documentele semnate sau sigilate se păstrează întotdeauna și în forma originală.

– utilizarea tehnologiilor pe termen lung se planifică (CEN/TS 18170, cl. 6.1): CERTDIGITAL ține un plan al tehnologiilor serviciului, revizuit cel puțin anual, odată cu verificarea formatelor (secțiunea 19.1), care cuprinde componentele sistemului AE și ale platformei, cu sfârșitul perioadei de suport și înlocuirea planificată a fiecăreia (secțiunea 19.3), înlocuirea de urgență a unei componente sau a sistemului, prin reluarea serviciului în centrul de date secundar ori din copiile de rezervă (secțiunea 20.7) și pe baza exportului complet, care nu

depinde de sistemul AE (secțiunea 16.4), precum și transformările planificate ale pachetelor și ale obiectelor: migrările de format și reînnoirile dovezilor (secțiunile 13.6 și 19.2).

6.8. Regăsirea, accesul și livrarea

– accesul la documentele arhivate este permis numai utilizatorilor autorizați de abonat sau de titularul dreptului de dispoziție, după autentificare, potrivit nivelului de clasificare și regimului de acces al documentului;

– documentele se pot căuta după metadate și se livrează ca pachete DIP care conțin documentul, metadatele, dovezile de arhivare și raportul de integritate (CEN/TS 18170, cl. 11);

– abonatul poate obține oricând exportul complet al arhivei sale sau exportul parțial al documentelor selectate, cu toate dovezile, într-un format documentat (secțiunea 16.4), pentru restituire sau pentru transferul la alt prestator (CEN/TS 18170, cl. 12);

– toate accesările, livrările și exporturile se jurnalizează.

6.9. Raportul de integritate la extragere

La fiecare extragere a unui document, beneficiarul autorizat primește automat un raport care confirmă că documentul beneficiază de prezumția de integritate de la începutul perioadei de păstrare până în momentul extragerii. Raportul este furnizat în mod fiabil și eficient, poartă sigiliul electronic calificat al serviciului și o marcă temporală calificată și poate fi verificat de orice parte care se bazează (art. 45j alin. (1) lit. (d) din Regulamentul eIDAS).

6.10. Perioada de păstrare și eliminarea

– perioada de păstrare se stabilește de abonat pentru fiecare tip de document sau document, inclusiv pe termen nelimitat, și se poate prelungi; CERTDIGITAL păstrează documentul cel puțin pe toată perioada stabilită;

– înainte de expirarea perioadei, titularul dreptului de dispoziție este notificat în mod repetat, iar după expirare are la dispoziție un termen în care poate prelungi păstrarea sau poate anula eliminarea (CEN/TS 18170, cl. 10.6): notificările se trimit cu 6 luni, 3 luni, o lună și o săptămână înainte de expirare, iar termenul de anulare de după expirare este de 7 zile;

– documentele nu se elimină cât timp există o obligație legală de păstrare, o cerere a unei autorități sau un litigiu cunoscut (blocare legală);

– eliminarea se aprobă de două persoane cu roluri de încredere diferite (principiul celor patru ochi), se face din toate copiile, inclusiv din copiile de rezervă, în termenul stabilit în secțiunea 18.4, prin metode care nu permit recuperarea, și se confirmă printr-un raport de eliminare cu sigiliul calificat al serviciului și cu marcă temporală calificată;

– metadatele minime ale documentelor eliminate și rapoartele de eliminare se păstrează ca dovadă.

6.11. Timpul de încredere și jurnalele

– evenimentele serviciului sunt datate cu o sursă de timp sincronizată cu UTC; atunci când se folosesc mărci temporale, acestea sunt **mărci temporale calificate**, emise de serviciul calificat de marcare temporală CERTDIGITAL (CEN/TS 18170, cl. 13.3.1; Regulamentul (UE) 2025/2532, anexa, lit. (i));

– se jurnalizează evenimentele critice și necritice ale serviciului (depuneri, respingeri, accesări, livrări, migrări, verificări de integritate, eliminări, operații administrative, evenimente de securitate), cu inițiatorul fiecărei operații, conform ETSI EN 319 401, cl. 7.10 (CEN/TS 18170, cl. 7.11 și 13.1–13.5);

– integritatea evenimentelor critice și a obiectelor digitale se protejează prin tehnici de semnătură digitală sau prin lanțuri de integritate (CEN/TS 18170, cl. 13.6);

– jurnalele se protejează împotriva modificării (jurnalele evenimentelor critice se sigilează periodic cu sigiliul serviciului și se marchează temporal) și se păstrează pe toată perioada de păstrare a documentelor la care se referă și cel puțin 10 ani de la încetarea contractului.

6.12. 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, inclusiv în domeniul arhivistic. Echipa care conduce activitățile tehnice și organizatorice ale serviciului include persoane cu competențe avansate în domeniul arhivistic și persoane cu competențe avansate în arhivarea electronică, în sensul Cadrului european al calificărilor și al clasificării ESCO (CEN/TS 18170, cl. 7.3). Pe lângă rolurile de încredere comune (Politicile generale, PG), serviciul folosește roluri proprii: operatorul de arhivă, responsabilul cu formatele și migrarea și aprobatorul eliminării, care nu poate fi aceeași persoană cu operatorul care execută eliminarea. Personalul primește cel puțin o dată la 12 luni instruire privind amenințările noi și practicile de securitate actuale (CEN/TS 18170, cl. 7.3; Regulamentul (UE) 2025/2532, anexa, lit. (d)).

6.13. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital și CEN/TS 18170, cl. 7 (organizare, gestionarea activelor, controlul accesului, securitate fizică, operare, gestionarea vulnerabilităților și a incidentelor, continuitate, conformitate, lanțul de aprovizionare), cu următoarele precizări:

– CERTDIGITAL aplică proceduri documentate de gestionare a informațiilor și a înregistrărilor privind procesele serviciului și acordurile cu abonații: contractele și anexele lor, acordurile de depunere, cererile titularilor dreptului de dispoziție, rapoartele serviciului și procesele-verbale se înregistrează, se protejează împotriva modificării și se păstrează conform secțiunii 6.11 (CEN/TS 18170, cl. 7.1);

– activele protejate de serviciu sunt pachetele de informații (SIP, AIP și DIP, secțiunea 4.1), împreună cu dovezile, rapoartele și jurnalele lor; ele se înscriu în inventarul activelor, cu proprietarul și clasificarea lor, iar suporturile pe care se păstrează se gestionează conform cerințelor de securitate a stocării și de integritate a AIP (capitolul 14 și secțiunea 19.3; CEN/TS 18170, cl. 7.4 și 10.4);

– CERTDIGITAL nu folosește subcontractanți pentru operarea serviciului; furnizorii de echipamente și programe sunt evaluați conform procedurii de achiziții (CEN/TS 18170, cl. 7.15);

– serviciul este operat în centrul de date principal și în centrul de date secundar, cu replicarea datelor arhivate și a jurnalelor, conform Procedurii DRP (PO_SI_63), cu durata maximă de restabilire de 24 de ore și pierderea maximă de date de cel mult 5 minute;

– copiile de rezervă, inclusiv copia offline păstrată în România, separat de ambele centre de date, sunt criptate, protejate la același nivel ca datele originale și se păstrează cel mult 90 de zile, iar restaurarea se testează cel puțin o dată la 6 luni, cu proces-verbal (ETSI EN 319 401, cl. 7.11.2);

– 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.

6.14. Controale criptografice și de rețea

– cheia privată a sigiliului serviciului se generează, se păstrează și se utilizează numai într-un dispozitiv calificat de creare a sigiliilor sau într-un modul 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 (Regulamentul (UE) 2025/2532, anexa, lit. (e));

– algoritmii criptografici se aleg și se monitorizează conform ECCG ACM; dacă un algoritm sau un parametru nu mai este adecvat, CERTDIGITAL actualizează politica sau creează un profil nou și ia măsuri pentru pachetele arhivate deja (reînnoirea dovezilor, secțiunea 6.5);

– componentele tehnice ale serviciului se autentifică reciproc, prin tehnici criptografice, înainte de a comunica;

– se aplică ETSI EN 319 401, cl. 7.8: scanarea de vulnerabilități cel puțin o dată pe trimestru, testul de penetrare cel puțin o dată pe an, iar firewall-urile blochează toate protocoalele și accesele care nu sunt necesare funcționării serviciului (CEN/TS 18170, cl. 7.9; Regulamentul (UE) 2025/2532, anexa, lit. (f)).

6.15. 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 (Regulamentul (UE) 2025/2532, anexa, lit. (b));

– pentru regimul național (secțiunea 4.5), CERTDIGITAL notifică ADR și orice dezvoltare sau modificare a sistemului AE și a procedurilor operaționale care ar putea afecta funcționarea și securitatea sistemului, cu descrierea modificării și a impactului ei, în cel mult 15 zile de la data la care devin operaționale (anexa nr. 2, art. 20 alin. (1), la normele tehnice aprobate prin Ordinul MCID nr. 20.717/2024); la încetare, ADR primește și notificarea de încetare a activității de administrator al arhivei electronice, iar fiecare abonat este înștiințat cu cel puțin 60 de zile înainte despre transferul arhivei și despre succesorul propus și poate refuza transferul (anexa nr. 1, art. 9, la aceleași norme);

– încetarea serviciului se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530 și revizuit cel puțin o dată la doi ani (CEN/TS 18170, cl. 7.13): pachetele arhivate, dovezile de arhivare și jurnalele se transferă, cu acordul abonaților, unui alt prestator de servicii de încredere calificat care prestează serviciul calificat de arhivare electronică, înscris cu acest serviciu într-o listă de încredere (art. 45j alin. (1) lit. (a) din Regulamentul eIDAS), și care, pentru arhivele supuse Legii nr. 135/2007, este și administrator de arhivă electronică acreditat de ADR (anexa nr. 1 la normele tehnice aprobate prin Ordinul MCID nr. 20.717/2024), ori unui alt prestator ales de abonat, sau se restituie abonaților prin export complet, cu toate dovezile și cu rapoartele de integritate (CEN/TS 18170, cl. 12; ISO 14721:2025, 3.3.6); documentele nu se elimină înainte de transfer sau restituire.

6.16. 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

– păstrează documentele pe toată perioada de păstrare, protejate împotriva pierderii și modificării, și le menține integritatea, confidențialitatea, lizibilitatea și dovada originii (art. 45j alin. (1) lit. (b) și (c));

– emite raportul de confirmare la depunere și raportul de integritate la fiecare extragere (art. 45j alin. (1) lit. (d));

– menține încrederea în semnăturile și sigiliile calificate din documentele arhivate (secțiunea 4.4);

– elimină documentele numai în condițiile secțiunii 6.10;

– restituie sau transferă arhiva la încheierea contractului sau la încetarea serviciului;

– publică documentația serviciului 24/7.

7.2. Obligațiile abonatului

– depune numai date și documente pe care are dreptul să le arhiveze, în formatele admise, cu metadatele cerute;

– păstrează originalele documentelor depuse cel puțin până la primirea raportului de confirmare a arhivării;

– stabilește corect perioadele de păstrare și desemnează titularii dreptului de dispoziție și utilizatorii autorizați;

– păstrează sub control exclusiv mijloacele de autentificare și notifică imediat CERTDIGITAL la suspiciunea de compromitere;

– 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 raportul de integritate 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 documentelor depuse; utilizarea serviciului peste limitările notificate în prealabil și recognoscibile de terți; nerespectarea

de către abonat a obligațiilor de la secțiunea 7.2; neverificarea de către partea care se bazează a raportului de integritate 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 calificat de arhivare electronică, 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 rapoartelor de integritate de către părțile care se bazează este gratuită.

8.2. Protecția datelor cu caracter personal

Pentru datele și documentele arhivate, 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 și pentru jurnalele serviciului, CERTDIGITAL este **operator**, conform Politicii de protecție a datelor (00d). CERTDIGITAL nu folosește persoane împuternicite pentru operarea serviciului. Drepturile persoanelor vizate privind datele din documentele arhivate se exercită față de abonat, în calitate de operator; CERTDIGITAL nu modifică, nu anonimizează și nu șterge documentele arhivate la cererea directă a persoanelor vizate, iar ștergerea unui document, decisă de abonat, se face numai prin eliminare, în condițiile secțiunilor 6.10 și 18.1. Ștergerea la cerere a datelor pentru care CERTDIGITAL este operator privește datele de cont și de contact; datele de identificare din jurnale și din rapoartele serviciului se păstrează pe durata de la secțiunea 6.11 (art. 17 alin. (3) lit. b) și e) din Regulamentul (UE) 2016/679). 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 și documentelor depuse, inclusiv drepturile de autor și celelalte drepturi de proprietate intelectuală; CERTDIGITAL dobândește numai dreptul de a le prelucra în măsura necesară prestării serviciului: stocarea, copierea în replică și în copiile de rezervă, schimbarea suportului și migrarea formatului în condițiile secțiunilor 6.7 și 19 (art. 45j alin. (1) lit. (c) din Regulamentul eIDAS), regăsirea, livrarea, exportul, transferul și eliminarea. Abonatul garantează că are dreptul să depună documentele și să acorde aceste drepturi (secțiunea 7.2). Restricțiile legale sau contractuale de utilizare a documentelor (de exemplu, confidențialitatea, drepturile de autor sau licențele) se exprimă prin nivelul de clasificare și regimul de acces din fișa de însoțire (secțiunea 12.2) și prin drepturile acordate de titularul dreptului de dispoziție și se aplică la fiecare acces (secțiunea 17.1); CERTDIGITAL nu folosește documentele în alt scop și nu le dezvăluie terților, cu excepția cazurilor prevăzute de lege (CEN/TS 18170, cl. 6.1 lit. f) și g) și cl. 6.4.2 lit. d)). 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) 2025/2532 și ale CEN/TS 18170

9.1. Tabel de corespondență

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 45i alin. (2)	prezumția de integritate și de acuratețe a originii	1.1
Regulamentul eIDAS, art. 45j alin. (1) lit. (a)	prestat de un prestator calificat; statut calificat	5.1
Regulamentul eIDAS, art. 45j alin. (1) lit. (b)	durabilitate și lizibilitate dincolo de perioada de valabilitate tehnologică	6.5, 6.7
Regulamentul eIDAS, art. 45j alin. (1) lit. (c)	protecție împotriva pierderii și modificării	6.5
Regulamentul eIDAS, art. 45j alin. (1) lit. (d)	raport automat de integritate, cu sigiliu calificat	6.9
Regulamentul (UE) 2025/2532, art. 1	semnături și sigilii calificate; păstrare calificată	4.4, 6.6
Regulamentul (UE) 2025/2532, anexa, lit. (a)	referințe normative (EN 319 401, EN 319 421, ISO 14721, ECCG ACM, EUCC)	2.1
Regulamentul (UE) 2025/2532, anexa, lit. (b) / CEN/TS 18170, cl. 6.1	politică și declarație de practici; notificări ADR (o lună / trei luni)	1.1, 6.1, 6.15
Regulamentul (UE) 2025/2532, anexa, lit. (c) / CEN/TS 18170, cl. 6.2	termeni și condiții	6.2
Regulamentul (UE) 2025/2532, anexa, lit. (d) / CEN/TS 18170, cl. 7.3	personal; instruire la 12 luni	6.12
Regulamentul (UE) 2025/2532, anexa, lit. (e) / CEN/TS 18170, cl. 7.6	confidențialitate; originea prin semnături sau sigilii calificate; chei în dispozitive certificate; ECCG ACM; autentificare reciprocă	6.3, 6.5, 6.14
Regulamentul (UE) 2025/2532, anexa, lit. (f) / CEN/TS 18170, cl. 7.9	securitatea rețelei; scanare trimestrială; test de penetrare anual; firewall	6.14
Regulamentul (UE) 2025/2532, anexa, lit. (g) / CEN/TS 18170, cl. 7.11	colectarea dovezilor (evenimente critice și necritice)	6.11
Regulamentul (UE) 2025/2532, anexa, lit. (h) / CEN/TS 18170, cl. 7.13	încetare; plan de încetare conform 2025/2530	6.15
Regulamentul (UE) 2025/2532, anexa, lit. (i) / CEN/TS 18170, cl. 13.3.1	timp de încredere; mărci temporale calificate	6.11
CEN/TS 18170, cl. 6.3–6.4	politica de securitate a informației; acordul de serviciu și acordul de depunere	6.2, 6.13
CEN/TS 18170, cl. 7.15	lanțul de aprovizionare; fără subcontractanți de operare	1.3, 6.13
CEN/TS 18170, cl. 8–9	pachetele de informații; SIP: formate, transmitere, primire, verificare	4.1, 6.3
CEN/TS 18170, cl. 10.2–10.4	AIP: generare, stocare, localizare, integritate	6.5
CEN/TS 18170, cl. 9.5, 10.2.5–10.2.6, 10.5	formatele admise; conversia formatelor; migrarea suporturilor	6.7
CEN/TS 18170, cl. 10.6	eliminarea	6.10
CEN/TS 18170, cl. 11–12	DIP; transferul la alt prestator	6.8, 6.15
CEN/TS 18170, cl. 13	trasabilitate; evenimente critice și necritice; protecția integrității	6.11
CEN/TS 18170, cl. 14	rapoarte	6.4, 6.9, 6.10

Cerință	Conținut	Secțiune
ISO 14721:2025 (OAIS)	comunitatea desemnată și baza ei de cunoștințe; acordul de depunere; modelul informațional: SIP, AIP, DIP, AIU și AIC, informația de conținut, informațiile de reprezentare, PDI, informațiile de împachetare și descriptive; obiectivele de păstrare	3.1, 4.1, 5.2, 6.2–6.10

Practicile detaliate pentru fiecare cerință sunt descrise în Partea a II-a, iar corespondența lor cu cerințele este în anexa A. Corespondența termenilor și a componentelor modelului OAIS cu prezentul document este în anexa B.

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. Identificarea documentului, participanții, referințele normative, definițiile și acronimele sunt cele din Partea I (capitolele 1–3). Capitolele 10–20 descriu practicile prin care se îndeplinesc cerințele din capitolul 6, capitolul 21 trimite la capitolele 7 și 8, anexa A arată corespondența practicilor cu cerințele Regulamentului de punere în aplicare (UE) 2025/2532 și ale CEN/TS 18170, iar anexa B, corespondența cu modelul de referință OAIS (ISO 14721:2025).

Serviciul se prestează prin sistemul electronic de arhivare AE (secțiunea 4.2), pe care CENTRUL DE CALCUL S.A. îl folosește și ca administrator de arhivă electronică, potrivit Legii nr. 135/2007 (secțiunea 4.5). Serviciul calificat se prestează numai din instanța sistemului AE găzduită în centrele de date ale CERTDIGITAL; instalările sistemului AE la sediul clienților nu fac parte din serviciu. Practicile din prezenta parte se aplică serviciului calificat (secțiunea 5.1).

10.1. Documentele publicate

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

– prezentul document, care conține și profilurile de arhivare (secțiunea 4.3);

– termenii și condițiile serviciului (TC-QEArch; secțiunea 11.1);

– lista formatelor admise (secțiunea 12.5) și lista codurilor de răspuns la depunere (secțiunea 12.6);

– specificația pachetelor de informații: pachetul depus, AIP și pachetul de export (secțiunea 12.2);

– conținutul și formatul rapoartelor emise de serviciu (raportul de confirmare, raportul de integritate și raportul de eliminare) și structura pachetului de export, descrise în prezentul document (secțiunile 12.7, 16.3, 16.4 și 18.5), precum și schemele XSD ale indexului pachetului de export și ale rapoartelor (secțiunea 16.4);

– certificatul calificat de sigiliu al serviciului (secțiunea 4.6) și instrucțiunile de verificare a rapoartelor (secțiunea 16.5);

– atestarea de conformitate a serviciului (secțiunea 20.11);

– documentele la care trimite prezentul document: Politicile generale CertDigital (PG), PSPPS, PDP-QTST și Planul de încetare a serviciilor (00r).

Modelul contractului de furnizare a serviciului nu se publică: se transmite solicitantului înainte de semnare, împreună cu termenii și condițiile serviciului (secțiunea 11.1).

10.2. Disponibilitatea depozitului și versiunile

Depozitul este disponibil 24/7, cu excepția intervențiilor planificate. Fiecare document se publică cu numărul versiunii și cu data intrării în vigoare, iar versiunile anterioare rămân disponibile în secțiunea „Arhivă” a depozitului. Prezentul document se revizuiește cel puțin anual și la orice schimbare semnificativă a serviciului. Modificările se aplică conform secțiunii 8.3, iar cele care afectează garanțiile oferite pentru documentele deja arhivate, conform secțiunii 5.3.

11. Accesul la serviciu

11.1. Contractarea serviciului

– înainte de încheierea contractului, solicitantul primește termenii și condițiile serviciului (TC-QEArch) și modelul contractului, care nu se publică (secțiunea 10.1), și are acces la prezentul document; clauzele privind răspunderea, perioadele de păstrare, eliminarea și restituirea arhivei se acceptă în mod expres (secțiunea 6.2);

– contractul cuprinde acordul de serviciu (profilurile, nivelul serviciului, perioadele de păstrare, accesul, raportarea, restituirea și transferul arhivei), acordul de depunere (formatele și metadatele pachetelor depuse, modul de transmitere, verificările la primire, codurile de răspuns și tratarea legăturilor către resurse externe, secțiunea 12.2) și clauzele prin care CERTDIGITAL acționează ca persoană împuternicită (secțiunea 8.2);

– la încheierea contractului, abonatul desemnează titularii dreptului de dispoziție și persoana care gestionează conturile și drepturile utilizatorilor săi; pentru arhivele supuse Legii nr. 135/2007, abonatul transmite nomenclatorul arhivistic, care se încarcă în sistem înainte de prima depunere.

11.2. Spațiul abonatului și rolurile utilizatorilor

Fiecare abonat are în sistemul AE un spațiu propriu, identificat prin codul de identificare fiscală, cu un director de stocare dedicat și cu o cotă de spațiu. Conturile utilizatorilor abonatului se creează numai în spațiul acestuia, cu următoarele roluri:

Rol	Ce poate face
titularul dreptului de dispoziție	aprobă și semnează depunerile, stabilește și modifică perioadele de păstrare, acordă accesul la documente, cere blocarea legală, anulează eliminarea
utilizatorul care depune	încarcă documentele și completează fișele de însoțire; nu poate finaliza arhivarea fără aprobarea titularului dreptului de dispoziție
utilizatorul autorizat	caută, consultă și extrage documentele, potrivit drepturilor acordate (secțiunea 17.1)

Drepturile se acordă de titularul dreptului de dispoziție sau de persoana desemnată de abonat în contract. Personalul CERTDIGITAL nu primește prin aceste roluri drepturi asupra conținutului documentelor (secțiunea 17.3).

11.3. Autentificarea

– utilizatorii se autentifică cu cel puțin doi factori sau cu certificat calificat (secțiunea 6.3); funcțiile titularului dreptului de dispoziție sunt disponibile numai după autentificarea cu certificat calificat;

– parolele au cel puțin 8 caractere și conțin majuscule, minuscule, cifre și caractere speciale; după resetare, parola se schimbă obligatoriu;

– conexiunile la serviciu folosesc HTTPS, cu TLS 1.2 sau superior (interfața web folosește TLS 1.3); accesul prin VPN se acordă numai cu acordul CERTDIGITAL.

11.4. Interfața web

Interfața web a sistemului AE permite încărcarea documentelor, completarea fișelor de însoțire, individual sau pentru mai multe documente deodată, aprobarea și semnarea depunerilor, căutarea, consultarea și extragerea documentelor și gestionarea perioadelor de păstrare și a drepturilor de acces. Titularul dreptului de dispoziție semnează din interfața web, cu certificatul său calificat: la distanță, prin serviciul calificat CERTDIGITAL de gestionare la distanță a dispozitivelor calificate de creare a semnăturilor electronice (PDP-rQSCD), după autentificarea sa în doi factori, conform acelui serviciu, sau local, cu propriul dispozitiv calificat de creare a semnăturilor; în aceeași operație se semnează fișa de însoțire, în format JAdES, și, pentru documentele PDF, documentul, în format PAdES (secțiunea 13.2). Adresa punctului de acces al serviciului calificat, https://arhivare.certdigital.ro, se publică în depozit și în termenii și condițiile serviciului (secțiunea 4.2).

11.5. Interfața de programare

– abonații își pot conecta sistemele de gestiune a documentelor la serviciu prin interfața de programare REST a sistemului AE, care permite verificarea conexiunii, calculul amprentei, încărcarea unuia sau a mai multor fișiere, cu fișele lor de însoțire, și semnarea;

– depunerile prin interfața de programare respectă aceleași reguli ca depunerile prin interfața web: aprobarea titularului dreptului de dispoziție sau sigiliul calificat al abonatului (secțiunea 12.3) și aceleași verificări (secțiunea 12.4);

– aplicațiile abonaților se autentifică prin TLS cu autentificare reciprocă, cu un certificat emis pentru abonat, și cu o cheie de acces; specificația interfeței se pune la dispoziția abonaților.

11.6. Limitele de utilizare

Cota de spațiu a fiecărui abonat, dimensiunea maximă a unui fișier și a unui pachet depus și numărul maxim de depuneri pe unitatea de timp se stabilesc în contract și se publică în termenii și condițiile serviciului. Depunerile care depășesc aceste limite se resping cu codul corespunzător (secțiunea 12.6), fără efect asupra documentelor deja arhivate. Cota de stocare a abonatului se stabilește tot prin contract.

12. Depunerea și acceptarea documentelor

12.1. Etapele depunerii

Depunerea se face prin interfața web sau prin interfața de programare și are următoarele etape:

– **încărcarea**: documentele ajung într-o zonă temporară a spațiului abonatului; ele nu sunt arhivate și nu beneficiază de garanțiile serviciului până la arhivare;

– **descrierea**: pentru fiecare document se completează fișa de însoțire (secțiunea 12.2), individual sau pentru mai multe documente deodată;

– **verificarea**: sistemul face verificările de la secțiunea 12.4;

– **aprobarea**: titularul dreptului de dispoziție semnează, cu certificatul său calificat, amprenta fiecărui document și fișa de însoțire, individual sau pentru mai multe documente deodată (secțiunea 12.3);

– **arhivarea**: sistemul atribuie identificatorul unic persistent, creează pachetul arhivat (AIP), cu dovezile de arhivare (capitolul 13), și emite raportul de confirmare (secțiunea 12.7).

12.2. Pachetul depus și metadatele obligatorii

Pachetul depus (SIP) cuprinde documentul sau documentele și fișa de însoțire. Fișa de însoțire conține:

Metadatele	Obligatorii
proprietarul (abonatul), emitentul documentului și titularul dreptului de dispoziție	da
tipul documentului	da
încadrarea în nomenclatorul arhivistic al abonatului	da, pentru arhivele supuse Legii nr. 135/2007 și Legii nr. 16/1996
data emiterii documentului	da
nivelul de clasificare și regimul de acces	da
formatul	da; se determină de sistem (secțiunea 12.5)
cuvintele-cheie	da
limba sau limbile documentului (codul ISO 639)	da
perioada de păstrare	da (secțiunea 18.1)
profilul de arhivare (1.3.6.1.4.1.47898.12.1.1 sau 1.3.6.1.4.1.47898.12.1.2)	da (secțiunea 4.3)
istoricul documentului	după caz
pentru documentele digitizate: originalul, metoda, dispozitivul, programul folosit și valoarea de original	da, pentru documentele digitizate

La arhivare, sistemul adaugă depunătorul (utilizatorul autentificat), identificatorul unic persistent al fiecărui obiect, localizarea, amprentele (secțiunea 13.1) și data și ora arhivării, în UTC.

Hiperlegăturile și trimiterile din documente către resurse externe (pagini web, alte documente sau date) fac parte din document și se păstrează ca atare. CERTDIGITAL nu verifică, nu descarcă și

nu arhivează resursele referite și nu garantează disponibilitatea lor. O resursă referită face parte din pachetul depus numai dacă abonatul o depune ca document separat, legat prin metadate de documentul care o referă (identificatorul unic persistent al documentului referit). Regula face parte din acordul de depunere (secțiunea 11.1; ISO 14721:2025, 2.6.3).

Formatul pachetelor de informații. CERTDIGITAL definește formatul, sintaxa și semnificația pachetelor de informații pe care le prelucrează serviciul (pachetul depus, AIP și pachetul de export) într-o specificație a pachetelor de informații, bazată pe specificațiile E-ARK (CSIP, SIP, AIP și DIP), cu METS pentru împachetare și PREMIS pentru informațiile de conservare, și publicată în depozit (secțiunea 10.1). Specificația descrie structura fiecărui pachet și componentele lui: informația de conținut, PDI, informațiile de împachetare și celelalte metadate. Formatul este definit într-un limbaj formal de definire a datelor (XML Schema), cu elementele obligatorii, cele opționale și regulile prin care un element opțional devine obligatoriu (de exemplu, metadatele documentelor digitizate). Fiecare pachet depus prin interfața de programare se validează automat față de această definiție, iar pentru depunerile prin interfața web, sistemul AE construiește pachetul în același format. Abonații care depun prin interfața de programare primesc specificația și exemple de pachete valide (CEN/TS 18170, cl. 8, 9.2, 9.3 și 10.2.1–10.2.2).

12.3. Stabilirea originii

– originea documentelor depuse se stabilește de CERTDIGITAL prin autentificarea depunătorului (secțiunea 11.3) și prin semnătura electronică calificată a titularului dreptului de dispoziție, aplicată pe amprenta documentului și pe fișa de însoțire; pentru depunerile automate prin interfața de programare, originea se poate stabili prin sigiliul electronic calificat al abonatului (Regulamentul (UE) 2025/2532, anexa, lit. (e));

– funcțiile titularului dreptului de dispoziție sunt disponibile numai după autentificarea cu certificat calificat; un utilizator fără certificat înregistrat în sistem nu poate finaliza o depunere;

– la fiecare depunere, semnătura sau sigiliul se validează conform Regulamentului de punere în aplicare (UE) 2025/1945: lanțul de certificare, starea certificatului la momentul semnării (OCSP sau CRL) și calificarea certificatului și a emitentului în Listele de încredere; depunerea se respinge dacă semnătura sau sigiliul nu este calificat sau nu este valid (secțiunea 12.6);

– rezultatul validării se păstrează în AIP.

12.4. Verificările la primire

Sistemul verifică fiecare pachet depus înainte de arhivare:

Verificarea	Dacă nu este îndeplinită
autentificarea depunătorului și dreptul lui de depunere în spațiul abonatului	respingere
formatul, sintaxa și structura pachetului depus, față de specificația pachetelor de informații (secțiunea 12.2), și existența tuturor obiectelor enumerate în pachet	respingere
completitudinea și corectitudinea fișei de însoțire	respingere
perioada de păstrare (în viitor sau permanentă)	respingere
dimensiunea fișierului (nenulă și în limitele de la secțiunea 11.6)	respingere
integritatea transferului: toate amprentele disponibile ale pachetului și ale fiecărui obiect, calculate de depunător înainte de transmitere, recalculate la primire	respingere
semnătura sau sigiliul care stabilește originea: concordanța cu amprenta documentului și validitatea (secțiunea 12.3)	respingere
identificarea și validarea formatului (secțiunea 12.5)	respingere sau, cu acordul abonatului, arhivare fără garantarea lizibilității
absența codului malițios	respingere
validarea semnăturilor și sigiliilor din document (Regulamentul de punere în aplicare (UE) 2025/1945)	profilul general: arhivare, cu rezultatul validării păstrat în AIP (rezultatele nedeterminate se marchează explicit); profilul cu păstrare calificată: respingere, dacă semnăturile sau sigiliile calificate nu sunt valide (secțiunea 15.1)

Rezultatul fiecărei verificări se documentează: pentru pachetele acceptate, în raportul de confirmare (secțiunea 12.7) și în AIP, iar pentru pachetele respinse, în jurnal, cu codul de răspuns și motivul (secțiunea 12.6; CEN/TS 18170, cl. 9.8.2).

CERTDIGITAL nu corectează pachetele depuse: un pachet care nu trece verificările se respinge, iar depunătorul îl retransmite corectat (CEN/TS 18170, cl. 9.8.1). Valorile completate automat de sistem în fișa de însoțire se marchează ca atare și se confirmă de depunător, iar fișa se aprobă prin semnătura titularului dreptului de dispoziție (secțiunea 12.3).

12.5. Formatele admise și regulile de conversie

CERTDIGITAL garantează lizibilitatea pe toată perioada de păstrare pentru următoarele formate (secțiunea 6.7):

Categoria	Formatele	Lizibilitatea
documente text și imagini de documente	PDF/A (ISO 19005)	garantată
date structurate	XML, cu schema asociată și cu descrierea câmpurilor (regulile de mai jos)	garantată
documente semnate sau sigilate	PAdES, XAdES, CAdES, JAdES și containere ASiC, cu documente în formatele din prezenta listă	garantată
imagini	TIFF, PNG, JPEG, JPEG 2000	garantată
text simplu și tabele	TXT și CSV, codificate UTF-8; pentru CSV, cu descrierea coloanelor (regulile de mai jos)	garantată

Categoria	Formatele	Lizibilitatea
alte formate	formatele enumerate în acordul de depunere (contractul, anexa 1), numai cu acordul abonatului	negarantată: se garantează numai integritatea, iar mențiunea se înscrie în raportul de confirmare

Lista de mai sus este lista formatelor admise. Pentru aceste formate, formatul identificat și specificația lui, împreună cu limba documentului (secțiunea 12.2) și, pentru XML și CSV, cu schema și descrierea câmpurilor (regulile de mai jos), sunt suficiente pentru ca documentele să fie înțelese de comunitatea desemnată, cu baza ei de cunoștințe (secțiunea 5.2; ISO 14721:2025, 4.3.2.3.1).

Corespondența dintre formatele de depunere și formatele de arhivare (CEN/TS 18170, cl. 10.2.6): fiecare format admis la depunere, inclusiv formatele enumerate în acordul de depunere, este și format de arhivare, deoarece fișierul primit se păstrează fără conversie (regulile de mai jos). Formatele-țintă ale migrării din timpul perioadei de păstrare sunt cele de mai jos; ele se aplică prin planul de migrare (secțiunea 19.2) și se publică în lista formatelor admise, cu corespondența „format inițial → format migrat”.

Formatele-țintă de conversie, folosite numai la migrarea din timpul perioadei de păstrare (capitolul 19), sunt (CEN/TS 18170, cl. 10.5.2): pentru PDF/A, o versiune ulterioară a PDF/A (ISO 19005); pentru XML, XML conform versiunii noi a schemei, cu schema și descrierea câmpurilor; pentru imagini, un format de imagine admis sau PDF/A; pentru TXT și CSV, aceleași formate, codificate UTF-8, cu descrierea coloanelor; pentru documentele semnate sau sigilate, versiunea migrată, nesemnată, a documentului conținut, într-un format admis, păstrată alături de original (secțiunea 19.2); pentru alte formate, formatul-țintă se stabilește cu abonatul. Formatul-țintă al fiecărui format admis se înscrie în registrul formatelor (secțiunea 19.1).

Regulile aplicate:

– formatul fiecărui fișier se identifică automat, după conținutul fișierului, nu după extensie sau după declarația depunătorului; pentru PDF/A se verifică și conformitatea cu specificația, iar pentru XML, conformitatea cu schema; formatul identificat se înscrie în registrul formatelor (secțiunea 19.1) și în AIP cu identificatorul lui din registrul PRONOM (PUID), dacă există (CEN/TS 18170, cl. 9.5);

– pentru documentele XML și CSV, abonatul depune, odată cu documentul sau o singură dată pentru tipul de document, schema (pentru XML) și descrierea semnificației câmpurilor sau a coloanelor; acestea se păstrează în AIP ca informații de reprezentare de structură și semantice (ISO 14721:2025, 4.3.2.3.2); dacă schema este publicată, abonatul poate indica adresa ei, iar CERTDIGITAL păstrează o copie a schemei în registrul formatelor (secțiunea 19.1) și o leagă de AIP; în lipsa schemei sau a descrierii, documentul se arhivează numai cu acordul abonatului, fără garantarea lizibilității (cod A01);

– CERTDIGITAL nu convertește și nu modifică documentele la depunere: fișierul primit se păstrează exact cum a fost primit, cu amprenta calculată la încărcare (secțiunea 13.1); semnătura titularului și sigiliul serviciului nu se aplică pe fișierul primit, ci pe fișa de însoțire și, pentru documentele PDF, pe versiunea de acces, obținută prin actualizare incrementală (secțiunea 13.5); dacă abonatul dorește arhivarea unui document într-un format admis, conversia se face de abonat înainte de depunere, iar abonatul poate depune ambele versiuni, legate prin metadate;

– documentele semnate sau sigilate se păstrează întotdeauna în forma originală;

– conversia documentelor arhivate, în timpul perioadei de păstrare, se face numai prin migrare (capitolul 19).

12.6. Confirmarea de primire și codurile de răspuns

La primirea fiecărui pachet, sistemul transmite automat depunătorului, imediat după încheierea încărcării, o confirmare de primire, cu un cod de răspuns (CEN/TS 18170, cl. 6.4.3 lit. c)). Pachetele acceptate se arhivează și primesc raportul de confirmare (secțiunea 12.7). Pachetele respinse nu se arhivează, iar depunătorul primește codul și motivul respingerii. Toate respingerile se jurnalizează (secțiunea 17.4).

Cod	Semnificația
A00	pachet acceptat și arhivat
A01	pachet acceptat; document într-un format din afara listei, arhivat cu acordul abonatului, fără garantarea lizibilității
A02	pachet acceptat în profilul general; semnături sau sigilii din document cu rezultat de validare negativ sau nedeterminat
R01	depunătorul nu este autentificat sau nu are drept de depunere
R02	metadate obligatorii lipsă sau incorecte
R03	perioadă de păstrare incorectă
R04	fișier gol, dimensiune peste limită sau cotă depășită
R05	amprenta nu corespunde: transfer incomplet sau modificat
R06	semnătura sau sigiliul care stabilește originea lipsește, nu este calificat sau nu este valid
R07	format neadmis, fără acordul abonatului pentru arhivarea fără garantarea lizibilității
R08	cod malițios detectat
R09	profilul cu păstrare calificată, cerut pentru un document fără semnături sau sigilii calificate valide ori într-un format neacceptat de QPS

Transferul și eșecurile de transfer. CERTDIGITAL răspunde de integritatea și confidențialitatea transferului pachetelor depuse prin interfața web sau prin interfața de programare, dacă depunătorul respectă procedura de depunere (secțiunile 11.3–11.5 și 12.1). Un transfer întrerupt, incomplet sau modificat nu produce o depunere: pachetul nu se arhivează, iar depunătorul primește, în interfața web sau în răspunsul interfeței de programare, codul de răspuns corespunzător (R04 sau R05) și reia transmiterea; un pachet pentru care depunătorul nu a primit confirmarea de

primire se consideră netransmis. Eșecurile de transfer se jurnalizează, iar eșecurile repetate sau cele cauzate de indisponibilitatea serviciului se tratează conform secțiunii 20.9, cu informarea abonatului (CEN/TS 18170, cl. 9.6 și 9.7).

Confirmarea de primire amintește depunătorului să păstreze originalele până la primirea raportului de confirmare (secțiunea 12.7). Fiecare depunere acceptată și fiecare respingere se înregistrează ca eveniment critic (secțiunea 17.4), iar neregulile constatate la depunere sau la stocare se comunică abonatului (CEN/TS 18170, cl. 9.7 și 10.1).

12.7. Raportul de confirmare a arhivării

– se emite automat pentru fiecare depunere acceptată (secțiunea 6.4), în cel mult 24 de ore de la aprobarea fișei de însoțire de către titularul dreptului de dispoziție; dacă un serviciu de care depinde arhivarea nu este disponibil, raportul se emite imediat după restabilire (secțiunea 13.4; CEN/TS 18170, cl. 6.4.3 lit. c)); raportul conține: identificatorul unic persistent și amprentele fiecărui obiect, profilul de arhivare, perioada de păstrare, rezultatul verificărilor de la depunere (inclusiv rezultatul validării semnăturilor și sigiliilor), depunătorul, titularul dreptului de dispoziție, identificatorul prezentului document (1.3.6.1.4.1.47898.12.1) și data și ora arhivării;

– se emite în format PDF, sigilat PAdES, și în format XML, sigilat XAdES, cu sigiliul calificat al serviciului și cu marcă temporală calificată (secțiunile 13.3 și 13.4);

– se transmite depunătorului și titularului dreptului de dispoziție și se păstrează în AIP; abonatul păstrează originalele cel puțin până la primirea raportului (secțiunea 7.2).

13. Integritatea și dovezile de arhivare

13.1. Amprentele criptografice

– la încărcare, sistemul calculează amprenta SHA-256 a fiecărui fișier; amprenta fișei de însoțire acoperă identificatorii, amprenta documentului și metadatele obligatorii;

– amprentele se înscriu în raportul de confirmare și în manifestul pachetului arhivat (secțiunea 13.5) și se recalculează la fiecare verificare a integrității (secțiunea 13.7);

– funcția hash se alege și se înlocuiește conform ECCG ACM (secțiunea 20.2).

13.2. Semnătura titularului dreptului de dispoziție

– titularul dreptului de dispoziție semnează fișa de însoțire, care conține amprenta documentului, cu semnătura sa electronică calificată, în format JAdES (ETSI TS 119 182-1), iar pentru documentele PDF semnează și versiunea de acces a documentului, în format PAdES (ETSI EN 319 142-1), prin actualizare incrementală (secțiunea 13.5); semnăturile se aplică în aceeași operație și se pot verifica independent de sistemul AE;

– semnătura se creează la distanță, prin serviciul calificat CERTDIGITAL de gestionare la distanță a dispozitivelor calificate de creare a semnăturilor electronice (PDP-rQSCD), sau local, cu propriul dispozitiv calificat de creare a semnăturilor al titularului (secțiunea 11.4);

– semnătura titularului se păstrează în AIP, împreună cu rezultatul validării ei (secțiunea 12.3);

– dovada de arhivare pentru terți este manifestul pachetului, sigilat cu sigiliul calificat al serviciului (secțiunile 13.3 și 13.5).

13.3. Sigiliul calificat al serviciului

– serviciul folosește un certificat calificat de sigiliu, emis pentru CENTRUL DE CALCUL S.A. și dedicat serviciului (secțiunea 4.6); cheia privată se află în modulul criptografic al serviciului (secțiunea 20.1);

– sigiliul se aplică pe rapoartele de confirmare, manifestele pachetelor arhivate, rapoartele de integritate, dovezile de migrare, rapoartele de eliminare, rapoartele de export, copiile și duplicatele eliberate din arhivă și pe sigiliile periodice ale jurnalelor, iar ca contrasemnătură, pe fișa de însoțire semnată de titular și pe versiunea de acces a documentelor PDF (secțiunile 13.2 și 13.5);

– sigiliul se creează în modulul criptografic al serviciului (secțiunea 20.1), în format PAdES pentru documentele și rapoartele PDF, JAdES pentru fișa de însoțire și XAdES pentru documentele XML și manifeste;

– marca temporală calificată, emisă de serviciul calificat de marcare temporală CERTDIGITAL, și datele de validare se adaugă prin serviciul de păstrare calificată CERTDIGITAL (QPS), în formatele de dovezi ale acestuia (PSPPS, secțiunea 3.3): augmentarea semnăturilor și a

sigiliilor la nivelul B-LTA sau înregistrări de dovezi (ERS, RFC 4998); un document nu se consideră arhivat, iar un raport sau o dovadă nu se emite, înainte de adăugarea mărcii temporale calificate (secțiunea 13.4); dovezile se mențin apoi conform secțiunii 13.6;

– cheia sigiliului nu se folosește în alte scopuri.

13.4. Mărcile temporale calificate și timpul de referință

– toate mărcile temporale folosite de serviciu sunt mărci temporale calificate, emise de serviciul calificat de marcare temporală CERTDIGITAL (PDP-QTST; secțiunea 6.11);

– dacă serviciul de marcare temporală nu este disponibil, operațiile care necesită marcă temporală se pun în coadă și se finalizează după restabilire; nu se emit rapoarte sau dovezi fără marcă temporală;

– serverele serviciului se sincronizează prin protocolul NTP cu serverele de timp ale CERTDIGITAL descrise în documentul „Sursa de timp” (00u), trasabile la UTC printr-un laborator UTC(k), conform cerințelor ETSI EN 319 421 privind sincronizarea ceasului cu UTC (CEN/TS 18170, cl. 13.3.1); abaterea se monitorizează, iar pierderea sincronizării se tratează ca incident (secțiunea 20.9); evenimentele se înregistrează în UTC.

13.5. Pachetul arhivat (AIP) și dovezile de arhivare

Fiecare AIP cuprinde (secțiunea 6.5):

– obiectele depuse, exact cum au fost primite, cu amprentele calculate la încărcare (secțiunea 13.1), și versiunile rezultate din migrare (capitolul 19), care constituie informația de conținut a pachetului (ISO 14721:2025, 4.3.2.4.2);

– pentru documentele PDF, versiunea de acces: o copie a documentului primit pe care se aplică, prin actualizare incrementală, semnătura PAdES a titularului dreptului de dispoziție și contrasemnătura serviciului (secțiunile 13.2 și 13.3); actualizarea incrementală lasă neschimbată revizia inițială, identică cu documentul primit, care rămâne verificabilă prin amprenta inițială; versiunea de acces se livrează utilizatorilor (secțiunea 16.2) și nu înlocuiește documentul primit;

– fișa de însoțire, semnată de titular și contrasemnată de serviciu (JAdES), și metadatele de păstrare: identificatorul unic persistent atribuit de sistem, care nu se reutilizează, profilul, perioada de păstrare și informațiile de reprezentare: formatul identificat și versiunea lui, specificația lui din registrul formatelor, limba documentului și, pentru XML și CSV, schema și descrierea câmpurilor (secțiunea 12.5);

– semnătura titularului dreptului de dispoziție și rezultatele validării semnăturilor și sigiliilor;

– raportul de confirmare;

– dovezile primite de la QPS: pentru toate documentele, cele care adaugă marca temporală calificată și datele de validare la semnăturile titularului și la sigiliul serviciului (secțiunea 13.3), iar pentru profilul cu păstrare calificată, și semnăturile din document augmentate (secțiunea 15.2);

– istoricul pachetului: verificările de integritate, reînnoirile dovezilor, migrările și blocările legale;

– informațiile despre transformarea pachetului depus în AIP: componentele pachetului depus preluate în AIP, inclusiv celelalte metadate din pachetul depus, cum sunt metadatele specifice tipului de document, amprentele lor la primire și în AIP, componentele adăugate la arhivare și data și ora arhivării; înainte de emiterea manifestului, amprentele componentelor din AIP se compară cu cele calculate la primire, iar o neconcordanță oprește arhivarea și se tratează ca incident (secțiunea 20.9; CEN/TS 18170, cl. 10.2.3 și 10.2.4);

– **manifestul pachetului**: lista tuturor componentelor de mai sus, cu identificatorul, formatul și amprenta fiecăreia, inclusiv corespondența dintre fiecare obiect depus și obiectele derivate din el (versiunea de acces, versiunile migrate), sigilată cu sigiliul calificat al serviciului și marcată temporal calificat (CEN/TS 18170, cl. 10.2.6).

Manifestul este dovada de arhivare a pachetului. La fiecare modificare a AIP, de exemplu după o migrare, după augmentarea semnăturilor și a sigiliilor sau după reînnoirea dovezilor (secțiunile 13.6 și 15.2), se emite un manifest nou, care cuprinde amprentele componentelor noi sau modificate și amprenta manifestului anterior (CEN/TS 18170, cl. 10.1).

Colecțiile. Fiecare document arhivat formează, cu componentele de mai sus, un AIP propriu, de tipul unitate de informații arhivate (AIU; ISO 14721:2025, 4.3.3.6). Compartimentele, pachetele și dosarele din structura arhivei abonatului și grupele de acces sunt colecții de acces (ISO 14721:2025, 1.6.2 și 4.3.3.9): se definesc numai prin descrierea lor (codul, denumirea, descrierea și unitatea căreia îi aparțin), nu au informații de împachetare și PDI proprii, iar încadrarea fiecărui document în ele se păstrează ca informație de context în AIP-ul documentului. Arhiva fiecărui abonat este o colecție de informații arhivate (AIC; ISO 14721:2025, 4.3.3.8), cu PDI proprii: proveniența (abonatul, contractul în baza căruia s-a constituit arhiva și data constituirii ei), criteriul și procesul de constituire (documentele depuse de abonat în spațiul său, prin depunerea descrisă în capitolul 12), contextul (nomenclatorul arhivistic și structura arhivei), referința (identificatorul spațiului abonatului, secțiunea 11.2), nivelul de securitate și drepturile de acces (nivelurile de clasificare, regimurile de acces și drepturile acordate de titularii dreptului de dispoziție, secțiunea 17.1) și fixitatea: inventarul AIP-urilor arhivei, cu amprentele manifestelor lor, care este și informația de împachetare a colecției, sigilat cu sigiliul calificat al serviciului și marcat temporal calificat la fiecare verificare periodică a integrității (secțiunea 13.7) și la fiecare export (secțiunea 16.4).

13.6. Reînnoirea dovezilor

– dovezile de arhivare (manifestele, rapoartele, semnăturile și sigiliile din AIP) se mențin verificabile prin adăugarea de mărci temporale calificate de arhivă, înainte de expirarea certificatelor pe care se bazează (certificatul sigiliului serviciului și certificatul serviciului de marcare temporală) și înainte ca algoritmii folosiți să devină nesiguri conform ECCG ACM (secțiunea 6.5);

– dacă funcția hash devine nesigură, amprentele obiectelor se recalculează cu o funcție nouă, iar noul manifest se sigilează și se marchează temporal înainte ca funcția veche să își piardă siguranța;

– reînnoirile se planifică pe baza unui registru al datelor de expirare și al pragurilor ECCG ACM, se execută automat și se înregistrează în istoricul AIP și în jurnale; eșecul unei reînnoiri se tratează ca incident (secțiunea 20.9).

Dovezile se reînnoiesc prin operația de augmentare a serviciului de păstrare calificată CERTDIGITAL, profilul AUG (1.3.6.1.4.1.47898.10.1.5).

13.7. Verificarea periodică a integrității

– integritatea fiecărui obiect se verifică prin recalcularea amprentelor și compararea lor cu amprentele înregistrate în jurnalul de audit la depunere (secțiunea 17.4) și cu manifestul și prin verificarea sigiliului și a mărcilor temporale ale manifestului: la fiecare extragere (secțiunea 16.3), după fiecare restaurare din copia de rezervă sau din replică și periodic, pentru toate obiectele din toate copiile, cu frecvența de la secțiunea 6.5 (CEN/TS 18170, cl. 14.1);

– fiecare verificare a integrității și rezultatul ei se înregistrează ca eveniment critic în jurnal (secțiunea 17.4) și în istoricul AIP, iar rezultatul verificării periodice, și într-un raport sigilat;

– exhaustivitatea arhivei se verifică zilnic, automat: numărul AIP-urilor create, al celor eliminate conform capitolului 18 și al celor existente în fiecare copie se compară cu inventarul arhivei fiecărui abonat (secțiunea 13.5); un rezultat conform se înregistrează ca eveniment necritic, iar o neconcordanță, ca eveniment critic, și se tratează ca incident (secțiunea 20.9; CEN/TS 18170, cl. 10.1);

– rapoartele de integritate se emit numai după verificarea integrității de mai sus (CEN/TS 18170, cl. 14.1);

– orice neconcordanță, pierdere sau corupere a datelor ori a metadatelor se tratează ca incident (secțiunea 20.9): obiectul afectat se restaurează dintr-o copie a cărei integritate a fost verificată, conform procedurii de restaurare documentate și testate (secțiunea 14.3), în cel mult 24 de ore de la detectare, iar evenimentul se înregistrează ca eveniment critic (secțiunea 17.4); abonatul este informat despre incident și, după restaurare, despre rezolvarea lui; dacă

nu există o copie validă, abonatul este informat, iar raportul de integritate indică situația (CEN/TS 18170, cl. 10.4 și 14.1);

– integritatea copiilor de rezervă se verifică și la reluarea activității după un dezastru, conform planului de continuitate (secțiunea 20.7).

14. Stocarea, replicarea și copiile de rezervă

14.1. Infrastructura și localizarea datelor

– sistemul AE este o aplicație web, cu două baze de date relaționale: una pentru registrul arhivei, fișele de însoțire, semnături și utilizatori și una, separată, pentru jurnalul de audit; fișierele arhivate se păstrează criptat în sistemul de fișiere, într-un director dedicat fiecărui abonat (secțiunea 14.4);

– serverele sunt mașini virtuale pe platforma de virtualizare a CERTDIGITAL, cu stocare distribuită;

– infrastructura se află în centrul de date principal al CERTDIGITAL, la sediul din Târgu Jiu, și în centrul de date secundar, situat tot în municipiul Târgu Jiu, la altă adresă;

– pentru ca AIP-urile să se afle permanent în cel puțin două locații îndepărtate geografic, o copie a fișierelor arhivate, a bazelor de date ale sistemului AE și a jurnalelor se păstrează și în locația CERTDIGITAL din București, prin replicarea asincronă a volumelor de stocare (secțiunea 14.2; CEN/TS 18170, cl. 10.4); până la punerea în funcțiune a acestei replici, riscul unui eveniment care afectează simultan ambele centre de date din Târgu Jiu se tratează prin analiza riscurilor comune și prin copia offline de la secțiunea 14.3, păstrată separat de ambele centre, cu riscul rezidual acceptat formal de conducere;

– în afara acestor locații, datele arhivate se păstrează numai în copia offline criptată de la secțiunea 14.3, într-o locație din România; datele arhivate nu părăsesc România și Uniunea Europeană (CEN/TS 18170, cl. 10.3);

– pentru acest serviciu, CERTDIGITAL nu folosește servicii de stocare sau de calcul ale terților (secțiunea 1.3).

– AIP-urile se păstrează numai în mediile de stocare ale serviciului; copii ale AIP-urilor nu se folosesc în medii de test, de dezvoltare sau în alte medii, inclusiv pentru testele de migrare (secțiunea 19.2), decât cu autorizarea scrisă a abonatului, înscrisă într-un registru al autorizărilor; în rest, testele se fac pe date de test (CEN/TS 18170, cl. 10.1).

14.2. Replicarea între centrele de date

– fișierele arhivate, ambele baze de date ale sistemului AE și jurnalele se replică din centrul de date principal în centrul de date secundar, prin replicarea asincronă, pe bază de instantanee, a volumelor de stocare; replica este a doua copie a arhivei, păstrată într-o clădire separată (secțiunea 6.5; ISO 14721:2025, 4.2.3.4);

– volumele care conțin aceste date se replică la cel mult 5 minute, ca volumele celorlalte servicii critice; celelalte componente ale sistemului se replică la cel mult 6 ore, iar configurația platformei de virtualizare se sincronizează orar;

– intervalul de replicare respectă obiectivul RPO al serviciului (secțiunea 20.7); starea și întârzierea replicării se monitorizează permanent, iar depășirea intervalului generează o alertă (secțiunea 20.6).

– fișierele arhivate, ambele baze de date ale sistemului AE și jurnalele se replică asincron, din centrul de date principal, și în locația CERTDIGITAL din București (secțiunea 14.1), cu monitorizarea stării și a întârzierii replicării, ca pentru centrul de date secundar (CEN/TS 18170, cl. 10.4);

– finalizarea stocării fiecărui AIP pe fiecare suport (centrul de date principal, replica din centrul de date secundar și copia offline, secțiunea 14.3) se înregistrează în istoricul AIP, cu data și ora; stocarea în centrul de date principal se confirmă abonatului prin raportul de confirmare (secțiunea 12.7), iar stocarea pe celelalte suporturi se poate consulta, pentru fiecare identificator de AIP, în interfața web și prin interfața de programare (CEN/TS 18170, cl. 10.1).

– replicarea și orice alt schimb de AIP-uri între centrele de date se fac numai prin canale de încredere, criptate și autentificate reciproc prin certificate (secțiunea 14.4; CEN/TS 18170, cl. 10.4);

– consistența AIP-urilor dintre toate copiile (centrele de date și locația din București) se verifică periodic, odată cu verificarea periodică a integrității (secțiunea 13.7), prin compararea inventarului AIP-urilor și a amprentelor manifestelor din fiecare copie; orice diferență se tratează ca incident (secțiunea 20.9) și se corectează dintr-o copie validă (CEN/TS 18170, cl. 10.4).

14.3. Copiile de rezervă și restaurarea

– mașinile virtuale ale sistemului, fișierele arhivate și configurația sistemului, inclusiv a serviciului de autentificare, se copiază zilnic; ambele baze de date au copii complete zilnice și arhivarea continuă a jurnalului tranzacțiilor, care permite restaurarea la un moment dat; eșecul unei copii generează o alertă;

– integritatea fiecărei copii se verifică automat după creare, iar o verificare eșuată se tratează ca incident (secțiunea 20.9; ETSI EN 319 401, REQ-7.11.2-03X);

– copiile de rezervă se păstrează în centrul de date secundar; în plus, o copie offline, actualizată cel puțin săptămânal, se păstrează separat de ambele centre de date, într-o locație din România cu acces controlat; fiind deconectată de rețea, copia offline este protejată împotriva modificării și a programelor malițioase (ETSI EN 319 401, REQ-7.11.2-02X lit. c); ISO 14721:2025, 4.2.3.4);

– copiile de rezervă, inclusiv copia offline, sunt protejate la același nivel ca datele originale: sunt criptate (AES-256), cu chei păstrate separat de copii, disponibile pentru restaurare și atunci când ambele centre de date sunt indisponibile; accesul la ele este restricționat la

personalul cu roluri de încredere, iar restaurarea se aprobă de ofițerul de securitate IT (secțiunea 17.3; ETSI EN 319 401, REQ-7.11.2-02X lit. d) și e));

– fiecare suport al copiei offline se înscrie în registrul copiilor externe al sistemului AE, cu numărul de ordine, eticheta, mediul de stocare, locația fizică și termenul de păstrare;

– toate copiile de rezervă, inclusiv copia offline, se păstrează cel mult 90 de zile; la expirare, copiile se șterg automat, iar suporturile offline se șterg securizat sau se distrug, cu proces-verbal, iar distrugerea se înscrie în registrul copiilor externe (secțiunea 18.4);

– restaurarea se testează cel puțin o dată la 6 luni, cu proces-verbal, iar cel puțin un test pe an se face din copia offline; integritatea datelor restaurate se verifică față de manifeste (secțiunea 13.7), iar constatările testelor se tratează prin măsuri corective (ETSI EN 319 401, REQ-7.11.2-04X).

14.4. Criptarea la stocare și confidențialitatea

– fișierele arhivate, bazele de date și copiile de rezervă se criptează la stocare, cu algoritmi conformi ECCG ACM; fișierele arhivate se criptează cu AES-256 în modul GCM, cu o cheie separată pentru fiecare abonat; cheile abonaților se păstrează numai învelite (criptate) cu o cheie care nu părăsește modulul criptografic, nu se afișează și nu se transmit prin interfețele sistemului, iar o cheie se schimbă numai cu re-criptarea fișierelor protejate de ea; cheile se distrug după eliminarea tuturor documentelor abonatului (secțiunea 18.4);

– comunicațiile cu utilizatorii și între componente folosesc TLS 1.2 sau superior (secțiunea 6.5);

– accesul la conținut este permis numai utilizatorilor autorizați de abonat (capitolul 17); personalul CERTDIGITAL nu consultă conținutul documentelor (secțiunea 17.3).

Datele arhivate se criptează la stocare cu AES-256, cu chei separate pentru fiecare abonat, gestionate în modulul criptografic.

15. Menținerea validității semnăturilor și sigiliilor calificate (profilul 1.3.6.1.4.1.47898.12.1.2)

15.1. Admiterea documentelor în profil

– în profilul cu păstrare calificată se arhivează numai documente care conțin semnături sau sigilii electronice calificate valide la depunere (secțiunea 6.3), în formatele acceptate de serviciul de păstrare calificată CERTDIGITAL (QPS): CAdES, XAdES, PAdES și ASiC-E (PSPPS, secțiunea 3.3);

– semnăturile și sigiliile se validează la depunere de QPS, conform politicii sale de validare, cu perioada de grație de 24 de ore pentru publicarea revocărilor (PSPPS, secțiunea 4.1); raportul de validare se păstrează în AIP;

– documentele care nu îndeplinesc aceste condiții se resping din profil (cod R09) și pot fi arhivate, la cererea abonatului, în profilul general.

Documentele JAdES nu se admit în profilul cu păstrare calificată până când serviciul de păstrare calificată acceptă acest format (PSPPS, secțiunea 3.3).

15.2. Utilizarea serviciului de păstrare calificată

– serviciul de arhivare este client al QPS, prin protocolul ETSI TS 119 512, în condițiile PSPPS (1.3.6.1.4.1.47898.10.1); CERTDIGITAL răspunde în ansamblu de serviciu (secțiunea 1.3);

– la arhivare, fiecare document semnat sau sigilat din profil se transmite QPS cu obiectivul de păstrare a semnăturilor (PDS); QPS validează semnăturile și sigiliile, colectează datele de validare și le aduce la nivelul LTA, iar semnăturile augmentate și dovezile se păstrează în AIP, alături de originalul depus, care nu se înlocuiește;

– în fiecare răspuns, QPS indică durata estimată de valabilitate a dovezilor și data recomandată pentru augmentarea următoare; serviciul de arhivare înregistrează aceste date în AIP și retransmite automat documentul și dovezile înaintea datei recomandate;

– dovezile primite de la QPS se includ în manifestul AIP (secțiunea 13.5), iar raportul de integritate indică ultimul eveniment de păstrare (secțiunea 16.3).

Sistemul AE folosește serviciul de păstrare calificată CERTDIGITAL cu profilul WOS (1.3.6.1.4.1.47898.10.1.1) la arhivare și cu profilul AUG (1.3.6.1.4.1.47898.10.1.5) la augmentare; până la punerea în funcțiune a versiunii G5 a serviciului de păstrare se folosește QPS G4, apoi versiunea G5.

15.3. Monitorizarea și evenimentele de păstrare

– serviciul ține evidența datelor recomandate pentru augmentare și a datelor de expirare ale certificatelor din dovezi; operatorul de arhivă primește alerte pentru augmentările nefinalizate;

– se declanșează augmentări suplimentare la publicarea unei versiuni a ECCG ACM care declară nesiguri algoritmii folosiți și la compromiterea cheii unei autorități de certificare sau de marcare temporală din lanțul dovezilor;

– dacă QPS nu este disponibil, cererile se reiau până la finalizare, înaintea datei recomandate; o augmentare nefinalizată la data recomandată se tratează ca incident (secțiunea 20.9).

15.4. Documentele semnate din profilul general

În profilul general, semnăturile și sigiliile din documente se validează la depunere, iar rezultatul se păstrează în AIP (secțiunea 12.4). Pentru semnăturile și sigiliile electronice calificate valide la depunere, încrederea se menține și în profilul general, prin serviciul de păstrare CERTDIGITAL, conform secțiunilor 15.2 și 15.3, cel puțin până la sfârșitul perioadei de păstrare (art. 1 alin. (1) din Regulamentul de punere în aplicare (UE) 2025/2532). Pentru celelalte semnături și sigilii (necalificate sau cu rezultat de validare negativ ori nedeterminat), CERTDIGITAL menține integritatea și dovada originii documentelor prin dovezile de arhivare (capitolul 13), dar nu menține validitatea semnăturilor și a sigiliilor după expirarea certificatelor pe care se bazează.

16. Regăsirea, livrarea și dovada integrității

16.1. Căutarea

Utilizatorii autorizați caută documentele după metadate și după expresii, precum și în textul documentelor, inclusiv în textul recunoscut optic (OCR), indexat în baza de date. Rezultatele cuprind numai documentele la care utilizatorul are drept de acces (secțiunea 17.1).

16.2. Livrarea documentelor și copiile

– la fiecare extragere (descărcare prin interfața web sau regăsire prin interfața de programare), utilizatorul autorizat primește pachetul livrat (DIP): documentul, exact cum a fost primit, și, după caz, versiunea de acces (secțiunea 13.5) și versiunile migrate, metadatele, dovezile de arhivare și raportul de integritate (secțiunea 16.3);

– pachetul livrat are structura pachetului de export de la secțiunea 16.4 (E-ARK DIP), limitată la AIP-urile sau la componentele cerute: o arhivă ZIP cu un index METS, conform specificației pachetelor de informații (secțiunea 12.2) și schemelor publicate, care descrie, pentru fiecare AIP inclus, identificatorul și componentele, cu formatul și amprenta fiecăreia; un pachet livrat poate cuprinde informații din unul sau mai multe AIP-uri (CEN/TS 18170, cl. 11);

– la cerere, CERTDIGITAL eliberează copii conforme și duplicate ale documentelor arhivate, sigilate cu sigiliul calificat al serviciului și marcate temporal calificat (secțiunea 13.3);

– utilizatorii autorizați pot imprima documentele; fiecare extragere, copie, duplicat sau imprimare se jurnalizează (secțiunea 17.4).

16.3. Raportul de integritate

– se generează automat la fiecare extragere și se livrează beneficiarului autorizat odată cu documentul, fără cost suplimentar (secțiunea 6.9); în plus, beneficiarul autorizat poate cere oricând pe durata perioadei de păstrare raportul de integritate al unui document, fără extragerea lui, prin interfața web sau prin interfața de programare, în condițiile din lista de tarife (CEN/TS 18170, cl. 14.1);

– conține: identificatorul documentului; amprentele înregistrate la arhivare și cele recalculate la extragere, cu data și ora verificării; rezultatul verificării manifestului (sigiliul și mărcile temporale); istoricul verificărilor periodice, al reînnoirilor și al migrărilor; profilul; data începerii perioadei de păstrare și intervalul acoperit, de la începutul perioadei de păstrare până la extragere; pentru profilul cu păstrare calificată, starea semnăturilor păstrate, după ultimul eveniment de păstrare al QPS; pentru celelalte documente semnate sau sigilate, rezultatul validării de la depunere (secțiunea 15.4) (CEN/TS 18170, cl. 14.1);

– confirmă că documentul beneficiază de prezumția de integritate de la începutul perioadei de păstrare până în momentul extragerii (art. 45j alin. (1) lit. (d) din Regulamentul eIDAS); dacă o verificare eșuează, raportul nu conține această confirmare și indică verificarea eșuată, iar evenimentul se tratează ca incident (secțiunea 20.9);

– se emite în format PDF (PAdES) și XML (XAdES), cu sigiliul calificat al serviciului și cu marcă temporală calificată.

– toate rapoartele serviciului (de confirmare, de integritate, de export și de eliminare) se pot folosi în afara sistemului AE și conțin cel puțin: identitatea serviciului (denumirea și identificatorul prezentului document, 1.3.6.1.4.1.47898.12.1); destinatarul raportului, atunci când este cunoscut; data și ora producerii raportului, atestate prin marca temporală calificată; identificatorii unici persistenți ai AIP-urilor vizate; tipul operației atestate; data operației, după caz (CEN/TS 18170, cl. 14.2).

16.4. Exportul complet și restituirea arhivei

– abonatul poate cere oricând, pentru restituire sau pentru transferul la alt prestator, exportul complet al arhivei sale sau exportul parțial al documentelor selectate după identificatori ori după metadate, de exemplu o clasă de documente sau o perioadă (secțiunea 6.8; CEN/TS 18170, cl. 12.1): exportul parțial cuprinde AIP-urile selectate, iar exportul complet, toate AIP-urile abonatului, cu obiectele, metadatele, dovezile, rapoartele și evenimentele critice din jurnale care privesc documentele exportate, împreună cu un raport de export sigilat, care enumeră conținutul și amprentele;

– pachetul de export are structura descrisă la sfârșitul prezentei secțiuni, publicată prin prezentul document (secțiunea 10.1), și conține schemele XML ale indexului și ale rapoartelor, astfel încât arhiva poate fi preluată de abonat sau de alt prestator fără sistemul AE (ISO 14721:2025, 5.4);

– exportul se livrează prin descărcare securizată sau pe suport criptat, după autentificarea persoanei desemnate de abonat;

– la încetarea contractului, arhiva rămâne disponibilă pentru consultare și export pe durata prevăzută în contract (30 de zile), după care documentele se elimină conform capitolului 18, cu raport de eliminare; documentele nu se elimină înainte de restituire sau de transfer, dacă abonatul le-a cerut în acest termen, și nici înainte ca abonatul sau prestatorul care preia arhiva să confirme formal primirea exportului, prin verificarea amprentelor din raportul de export (secțiunea 20.10; CEN/TS 18170, cl. 12.2.3); până la confirmare, abonatul este notificat în mod repetat, iar păstrarea arhivei după termenul de 30 de zile se face în condițiile din lista de tarife.

Exportul complet se face ca un pachet livrat conform specificației E-ARK DIP: o arhivă ZIP cu un index METS și cu informațiile de conservare în PREMIS (specificația pachetelor de informații,

secțiunea 12.2); indexul METS descrie structura AIP; după încetarea contractului, arhiva rămâne disponibilă pentru consultare și export 30 de zile. Arhiva ZIP cuprinde: câte un director pentru fiecare AIP, denumit după identificatorul unic persistent al documentului, cu toate componentele AIP (secțiunea 13.5); indexul METS, care enumeră, pentru fiecare AIP, identificatorul, profilul, perioada de păstrare, formatul, limba, componentele și amprentele lor; schemele XML ale indexului și ale rapoartelor; PDI-ul arhivei abonatului, cu nomenclatorul arhivistic, structura arhivei și drepturile de acces (secțiunea 13.5); extrasele din jurnale care privesc documentele abonatului, în format PREMIS (secțiunea 17.5); raportul de export, sigilat cu sigiliul calificat al serviciului și marcat temporal calificat, care enumeră conținutul și amprentele.

Interfața și procedura de transfer. Exportul se cere de persoana desemnată de abonat, după autentificare, din interfața web sau prin interfața de programare (secțiunile 11.4 și 11.5); funcția de export este disponibilă numai utilizatorilor cu drept de export (secțiunea 17.1) și operatorului de arhivă (secțiunea 20.3). Pachetul de export folosește numai formate deschise, documentate public: ZIP, XML 1.0 codificat UTF-8 (indexul METS și informațiile de conservare PREMIS, conform E-ARK DIP), cu schemele XSD ale indexului și ale rapoartelor, publicate în depozit (secțiunea 10.1) și incluse în pachet, și formatele documentelor arhivate (secțiunea 12.5), astfel încât poate fi preluat de un sistem nou sau de alt prestator fără sistemul AE (CEN/TS 18170, cl. 12.2.3 și 12.2.4). Pentru fiecare export complet și pentru fiecare transfer la alt prestator, operatorul de arhivă întocmește un program al operațiunilor, cu etapele, termenele, persoanele și competențele necesare și operațiunile de întreținere aferente, iar primirea se confirmă formal prin verificarea amprentelor din raportul de export (secțiunea 20.10). CERTDIGITAL răspunde de transfer: cerințele lui se identifică, se documentează, se proiectează, se implementează, se testează și se mențin pe toată durata serviciului; funcția de export se testează cel puțin o dată pe an și după fiecare schimbare semnificativă a sistemului AE, pe un abonat de test, prin preluarea exportului într-un mediu separat și verificarea amprentelor și a schemelor, cu proces-verbal; specificația exportului și procedura de transfer se actualizează la fiecare schimbare a sistemului AE care le afectează (CEN/TS 18170, cl. 12.2.4 și 12.3).

16.5. Verificarea de către părțile care se bazează

– partea care se bazează verifică sigiliul calificat și marca temporală calificată de pe raportul de integritate cu orice validator conform Regulamentului de punere în aplicare (UE) 2025/1945 care folosește Listele de încredere, de exemplu cu serviciul calificat de validare CERTDIGITAL, disponibil gratuit la https://ca.certdigital.ro/vs/;

– verifică statutul calificat al serviciului în Lista de încredere a României, la https://trustedlist.adr.gov.ro/ (secțiunea 7.3);

– poate recalcula amprenta documentului primit și o poate compara cu amprenta din raport;

– verificarea rapoartelor este gratuită (secțiunea 8.1).

17. Controlul accesului și jurnalizarea

17.1. Modelul de autorizare

– accesul se acordă pe roluri, cu drepturi la nivel de meniu, de tip de obiect, de câmp și de operație, după principiul privilegiului minim;

– fiecare document are un nivel de clasificare și un regim de acces; accesul se poate restrânge la grupuri de utilizatori, iar câmpurile protejate se maschează;

– accesul temporar se acordă pe bază de cerere aprobată, cu expirare (o zi sau o lună), ori prin acces protejat cu parolă, limitat în timp sau pe bază de jeton;

– drepturile se acordă de titularul dreptului de dispoziție sau de persoana desemnată de abonat (secțiunea 11.2); orice acordare sau retragere de drepturi se jurnalizează;

– nivelul de clasificare servește controlului accesului în cadrul abonatului; serviciul nu este destinat informațiilor clasificate în sensul legislației privind protecția informațiilor clasificate.

Serviciul nu arhivează informații clasificate.

17.2. Gestionarea conturilor

– conturile se creează, se modifică și se închid pe bază de formular aprobat; conturile sunt nominale și nepartajate;

– conturile închise se dezactivează și se păstrează, împreună cu jurnalele care le privesc, cel puțin pe durata de păstrare a jurnalelor (secțiunea 17.5);

– conturile privilegiate ale personalului CERTDIGITAL se revizuiesc cel puțin anual, cu proces-verbal (Politicile generale, secțiunea 6.2).

17.3. Accesul personalului CERTDIGITAL

– personalul CERTDIGITAL are acces la sistem numai prin conturi administrative nominale, cu autentificare cu cel puțin doi factori (Politicile generale, secțiunea 6.3), și numai pentru operațiile cerute de rolul său;

– operatorul de arhivă execută operațiile cerute de abonat (de exemplu, exporturile) și eliminările aprobate, fără drept de a modifica documentele arhivate;

– administratorii de sistem administrează infrastructura fără să consulte conținutul documentelor; accesul la conținut în scopuri tehnice, de exemplu la o restaurare, se face numai cu aprobarea ofițerului de securitate IT și se jurnalizează;

– orice modificare a unui document arhivat sau a dovezilor lui se detectează la verificarea integrității (secțiunea 13.7).

17.4. Evenimentele jurnalizate

– se jurnalizează evenimentele de la secțiunea 6.11, cu inițiatorul, data și ora (UTC) și rezultatul fiecărei operații; inițiatorul este utilizatorul autentificat (identificatorul contului și adresa IP) sau, pentru operațiile automate, procesul sistemului AE care a generat evenimentul, marcat explicit ca proces automat (CEN/TS 18170, cl. 13.3.2);

– **evenimentele critice**, care privesc integritatea, lizibilitatea sau regulile de acces ale pachetelor, formează jurnalul de audit (CEN/TS 18170, cl. 13.2 și 13.5): a) depunerea, cu amprenta fiecărui obiect; b) conversia formatului, la depunere sau în perioada de păstrare, cu amprentele obiectului înainte și după conversie; c) adăugarea sau modificarea metadatelor descriptive, tehnice și administrative, inclusiv a perioadei de păstrare și a blocărilor legale; d) livrarea pachetelor, exportul și transferul către abonat sau către alte destinații autorizate; e) neconcordanțele constatate la verificările de integritate sau de exhaustivitate; f) schimbarea algoritmilor criptografici și reînnoirea dovezilor; g) crearea, modificarea și dezactivarea conturilor utilizatorilor; h) acordarea, modificarea și retragerea drepturilor și a rolurilor; i) schimbarea sau revocarea mijloacelor de autentificare gestionate de serviciu; j) eliminarea, restaurarea din copiile de rezervă și orice altă operație care poate afecta integritatea;

– **evenimentele necritice** cuprind cel puțin (CEN/TS 18170, cl. 13.4): verificările reușite ale integrității și exhaustivității obiectelor; verificările reușite ale integrității și exhaustivității jurnalului de audit; încercările de autentificare și deschiderea și închiderea sesiunilor; accesul la pachete sau la părți ale lor (metadatele, fișa de însoțire, obiectele, rezultatele căutărilor); în plus, respingerile depunerilor, operațiile administrative și evenimentele de securitate;

– un eveniment critic se înregistrează înaintea confirmării operației; dacă evenimentul nu poate fi înregistrat, operația nu se execută, iar eșecul generează o alertă (de exemplu, o eliminare care nu poate fi jurnalizată nu se face) (CEN/TS 18170, cl. 13.5);

– sistemul AE înregistrează în baza de date istoricul modificărilor (utilizatorul, data, operația, câmpul, valoarea veche și valoarea nouă) și istoricul accesărilor (utilizatorul, adresa IP, data, documentul și tipul de acces); jurnalul nu poate fi modificat din aplicație;

– evenimentele sistemelor de operare ale serverelor se colectează centralizat.

17.5. Protecția și păstrarea jurnalelor

– jurnalul de audit (evenimentele critice, secțiunea 17.4) se ține separat pentru fiecare abonat, astfel încât fiecare abonat își poate accesa și urmări jurnalul independent de ceilalți abonați (CEN/TS 18170, cl. 13.3.3 și 13.6.3); jurnalul de audit al fiecărui abonat se înlănțuie (fiecare înregistrare conține amprenta înregistrării anterioare) și se sigilează zilnic cu sigiliul calificat al serviciului, cu marcă temporală calificată (secțiunea 6.11; CEN/TS 18170, cl. 13.6);

– lanțul și sigiliile periodice ale jurnalului de audit se verifică automat, zilnic și la cerere, pentru integritate și exhaustivitate (nicio înregistrare modificată, adăugată sau ștearsă); rezultatul

verificării se jurnalizează (secțiunea 17.4), iar o neconcordanță se tratează ca incident (secțiunea 20.9);

– sigiliile periodice ale jurnalelor se mențin verificabile pe toată durata de păstrare a jurnalelor, prin reînnoirea dovezilor (secțiunea 13.6);

– jurnalul de audit se păstrează cu același nivel de securitate ca pachetele arhivate la care se referă: criptare la stocare, acces numai pentru rolurile autorizate, replicare și copii de rezervă (capitolul 14; CEN/TS 18170, cl. 13.5);

– structurile de jurnal ale serviciului sunt: jurnalul de audit al fiecărui abonat, cu sigiliile sale periodice; jurnalul evenimentelor necritice; jurnalele sistemelor de operare ale serverelor, colectate centralizat (secțiunea 17.4);

– jurnalele se exportă în format XML conform modelului PREMIS 3 (evenimente și agenți), cu schema XML furnizată împreună cu exportul (secțiunea 16.4), utilizabil în afara sistemului AE; datele și orele se exprimă în UTC, în formatul ISO 8601 (CEN/TS 18170, cl. 13.3.1 și 13.5);

– jurnalele se replică și se copiază la fel ca arhiva (capitolul 14) și se păstrează pe toată perioada de păstrare a documentelor la care se referă și cel puțin 10 ani de la încetarea contractului;

– jurnalele se pun la dispoziția organismului de evaluare a conformității și a ADR; abonatul primește, la cerere, extrasul din jurnal privind documentele sale.

Jurnalele evenimentelor critice se înlănțuie și se sigilează zilnic.

18. Perioadele de păstrare și eliminarea

18.1. Stabilirea și modificarea perioadei de păstrare

– perioada de păstrare se preia din nomenclatorul arhivistic al abonatului (în ani, luni sau zile) sau se stabilește ca permanentă și se poate modifica pentru fiecare document (secțiunea 6.10);

– perioada de păstrare începe, pentru documentele încadrate în nomenclatorul arhivistic (arhivele supuse Legii nr. 16/1996 și Legii nr. 135/2007), la 1 ianuarie a anului următor celui în care a fost emis documentul, iar pentru celelalte documente, la data arhivării; data de început se înscrie în raportul de confirmare și în raportul de integritate (secțiunile 12.7 și 16.3; CEN/TS 18170, cl. 6.4.3 lit. k));

– perioada se stabilește și se modifică numai de titularul dreptului de dispoziție, după autentificarea cu certificat calificat; prelungirea este oricând posibilă, iar orice modificare se jurnalizează și se înscrie în istoricul AIP;

– un document se elimină numai după expirarea tuturor termenelor legale de păstrare care i se aplică și numai prin fluxul de eliminare de la secțiunile 18.2–18.5, fără ștergeri directe în sistem: la expirarea perioadei de păstrare stabilite, la încetarea contractului, după termenul de export (secțiunea 16.4), sau la cererea titularului dreptului de dispoziție;

– titularul dreptului de dispoziție poate cere, după autentificarea cu certificat calificat, eliminarea unui document înainte de expirarea perioadei stabilite, cu indicarea motivului; cererea echivalează cu modificarea perioadei de păstrare de către titular, se înregistrează, împreună cu motivul ei, ca eveniment critic (secțiunea 17.4) și urmează același flux ca eliminarea la expirare: se verifică dreptul solicitantului asupra documentului, termenele legale de păstrare (inclusiv cele din nomenclatorul arhivistic al abonatului) și blocările legale; documentul trece în starea „de eliminat” pe durata termenului de anulare de 7 zile (secțiunea 6.10); lista se aprobă de aprobatorul eliminării și se execută de operatorul de arhivă (secțiunea 18.4); ștergerea se face din toate copiile, iar eliminarea se confirmă prin raportul de eliminare (secțiunea 18.5); cererea care nu îndeplinește aceste condiții se respinge motivat, iar respingerea se jurnalizează (CEN/TS 18170, cl. 10.6).

18.2. Notificările înainte de expirare

– titularul dreptului de dispoziție este notificat prin e-mail și în interfața serviciului, în mod repetat, înainte de expirarea perioadei de păstrare, conform calendarului de la secțiunea 6.10;

– după expirare, documentul rămâne în starea „de eliminat” pe durata termenului de anulare; în acest termen, titularul poate prelungi păstrarea sau poate anula eliminarea;

– dacă titularul nu reacționează, eliminarea continuă conform secțiunii 18.4.

18.3. Blocarea legală

– blocarea legală se aplică unui document sau unui set de documente la cererea titularului dreptului de dispoziție ori, cu informarea abonatului, la cererea unei autorități sau la cunoașterea unui litigiu (secțiunea 6.10);

– cât timp blocarea este activă, documentul nu se elimină, chiar dacă perioada de păstrare a expirat;

– aplicarea și ridicarea blocării se jurnalizează, cu motivul și inițiatorul, și se înscriu în istoricul AIP.

18.4. Aprobarea și executarea eliminării

– lista documentelor de eliminat se generează automat după expirarea termenului de anulare și se aprobă de aprobatorul eliminării; eliminarea se execută de operatorul de arhivă, care nu poate fi aceeași persoană cu aprobatorul (secțiunile 6.10 și 6.12);

– documentul și toate componentele AIP-ului său care îi reproduc conținutul (versiunea de acces, versiunile migrate, textul indexat pentru căutare și obiectele păstrate de QPS) se șterg din stocarea principală, din bazele de date și din replică prin metode care nu permit recuperarea (suprascriere sau distrugerea cheii de criptare); după eliminare, documentul nu mai poate fi găsit prin căutare și nici extras;

– fiecare eliminare se înregistrează ca eveniment critic în jurnal (secțiunea 17.4; CEN/TS 18170, cl. 10.6);

– din copiile de rezervă, inclusiv din copia offline, documentul dispare la expirarea retenției acestora: copiile se șterg automat, iar suporturile offline se șterg securizat sau se distrug, cu proces-verbal (secțiunea 14.3); eliminarea din toate copiile, inclusiv din copiile de rezervă, se încheie în cel mult 90 de zile de la aprobarea eliminării (durata maximă de păstrare a copiilor de rezervă);

– dacă, în acest interval, sistemul se restaurează dintr-o copie de rezervă, eliminările aprobate după data copiei se reaplică înaintea reluării accesului la documente, pe baza rapoartelor de eliminare și a jurnalelor, iar reaplicarea se jurnalizează (secțiunea 20.7);

– intrarea din registrul arhivei se păstrează, cu data eliminării, împreună cu metadatele minime ale documentului eliminat (secțiunea 18.5).

18.5. Raportul de eliminare

– pentru fiecare eliminare se emite, după ștergerea din toate copiile, inclusiv din copiile de rezervă (secțiunea 18.4), un raport de eliminare, cu sigiliul calificat al serviciului și cu marcă temporală calificată, care conține identificatorii și amprentele documentelor eliminate, metadatele lor minime, temeiul eliminării (expirarea perioadei de păstrare, încetarea contractului sau cererea titularului dreptului de dispoziție), referința ordinului inițial de

eliminare (cererea titularului dreptului de dispoziție sau, la expirare, perioada de păstrare stabilită de acesta și lista de eliminare aprobată), data ordinului, autorul lui și, pentru eliminarea la cerere, motivul cererii, rezultatul verificării termenelor legale de păstrare și a blocărilor legale, aprobările, data efectivă a ștergerii din fiecare copie și copiile din care s-a făcut ștergerea (CEN/TS 18170, cl. 14.1);

– raportul se transmite titularului dreptului de dispoziție și se păstrează, împreună cu metadatele minime, cel puțin cât jurnalele (secțiunea 17.5).

– dacă se cere un document eliminat, solicitantul autorizat primește, în locul documentului, raportul de eliminare sau o informare întocmită pe baza jurnalului, cu data și temeiul eliminării (CEN/TS 18170, cl. 10.6).

19. Lizibilitatea și migrarea

19.1. Monitorizarea formatelor

– responsabilul cu formatele și migrarea (secțiunea 6.12) ține registrul formatelor admise și verifică, cel puțin anual, viabilitatea fiecărui format: stadiul specificației, suportul în programele larg folosite și riscul de învechire, cu estimarea orizontului în care formatul poate deveni depășit; rezultatul fiecărei revizuiri se înscrie în registrul formatelor, cu data revizuirii și data următoarei revizuiri (CEN/TS 18170, cl. 10.5.2);

– dacă un format devine riscant, el se elimină din lista formatelor admise pentru depunerile noi, iar lista actualizată se publică (secțiunea 10.1); pentru documentele deja arhivate se întocmește un plan de migrare (secțiunea 19.2).

19.2. Migrarea formatelor

– migrarea se face pe baza unui plan aprobat, după teste pe un eșantion, cu informarea abonaților afectați cu cel puțin 30 de zile înainte (secțiunea 6.7; CEN/TS 18170, cl. 6.4.3 lit. h));

– după conversie se verifică automat păstrarea proprietăților semnificative ale documentului, definite pentru fiecare format în registrul formatelor (secțiunea 19.1) și, după caz, în acordul de depunere (de exemplu, numărul de pagini, textul și aspectul) (CEN/TS 18170, cl. 10.2.5);

– originalul se păstrează întotdeauna, iar legătura dintre original și versiunea migrată se înregistrează în AIP;

– pentru fiecare migrare se emite o dovadă de migrare, sigilată și marcată temporal, care conține identificatorii și amprentele originalului și ale versiunii migrate, formatul vechi și formatul nou, instrumentul folosit, versiunea și parametrii acestuia și avertizările emise la conversie, precum și un manifest nou al AIP (secțiunea 13.5);

– metoda de conversie și fiecare conversie, cu formatul vechi, formatul nou, instrumentul și avertizările conversiei, se înregistrează ca evenimente critice în jurnal (secțiunea 17.4; CEN/TS 18170, cl. 10.5.2 și 13.2);

– pentru documentele semnate sau sigilate, migrarea produce o versiune nouă, nesemnată, păstrată alături de original; originalul semnat se păstrează întotdeauna, iar validitatea semnăturii se menține conform capitolului 15.

19.3. Migrarea suporturilor și a platformei

– suporturile de stocare și echipamentele se înlocuiesc înainte de sfârșitul perioadei lor de suport; datele se copiază cu verificarea amprentelor fiecărui obiect față de manifeste (secțiunea 13.7), fără modificarea dovezilor;

– schimbările platformei (sistemul de operare, baza de date, aplicația) se fac prin procesul de gestionare a schimbărilor (Politicile generale, secțiunea 9.1), cu teste și cu plan de revenire;

– fiecare migrare se jurnalizează și se înscrie în istoricul AIP-urilor afectate.

20. Controale operaționale

20.1. Cheile serviciului și modulele criptografice

– cheia privată a sigiliului serviciului se generează într-o ceremonie, sub control dual, cu proces-verbal, în modulele criptografice ale generației G5 (Thales Luna; Politicile generale, secțiunea 7.1), certificate conform secțiunii 6.14 și configurate conform certificării;

– cheia nu părăsește modulul în clar; copiile ei de rezervă sunt criptate și pot fi restaurate numai într-un modul certificat, sub control dual;

– datele de activare ale cheii sunt deținute numai de persoane cu roluri de încredere și nu se păstrează în aplicație;

– pentru sigilarea rapoartelor și a dovezilor nu se folosesc chei sau certificate păstrate în fișiere;

– certificatul se reînnoiește înainte de expirare; la sfârșitul utilizării, cheia se distruge sub control dual, cu proces-verbal.

20.2. Algoritmii criptografici

– algoritmii și lungimile cheilor respectă ECCG ACM: amprente SHA-256 sau mai puternice; semnături și sigilii RSA sau ECDSA, cu lungimile de cheie admise; TLS 1.2 sau superior, cu suitele admise; sistemul AE folosește SHA-256 pentru amprente și RSA-SHA256 pentru semnături;

– algoritmul și lungimea cheii sigiliului serviciului se publică împreună cu certificatul (secțiunea 10.1);

– ofițerul de securitate IT ține inventarul algoritmilor și al parametrilor folosiți, în trecut și în prezent, în pachetele arhivate, în dovezile și în sigiliile serviciului, urmărește publicarea versiunilor noi ale ECCG ACM, ținând seama și de ETSI TS 119 312, și reevaluează algoritmii din inventar cel puțin anual și la fiecare versiune nouă a ECCG ACM, cu proces-verbal; dacă un algoritm sau un parametru nu mai este adecvat, se aplică secțiunea 6.14 (profil nou, după caz, și reînnoirea dovezilor, secțiunea 13.6) (CEN/TS 18170, cl. 7.6; Regulamentul (UE) 2025/2532, anexa, lit. (e)).

20.3. Personalul și rolurile de încredere

– personalul cu roluri de încredere este angajat al CENTRUL DE CALCUL S.A. și este verificat, numit și instruit conform Politicilor generale (capitolul 5);

– rolurile proprii serviciului sunt:

Rol	Responsabilități	Incompatibilități
operatorul de arhivă	asistența abonaților la depunere, blocările legale cerute, exporturile, executarea eliminărilor aprobate, urmărirea augmentărilor	nu aprobă eliminările pe care le execută

Rol	Responsabilități	Incompatibilități
responsabilul cu formatele și migrarea	lista și registrul formatelor, monitorizarea lor, planurile și dovezile de migrare	—
aprobatorul eliminării	aprobarea listelor de eliminare și verificarea rapoartelor de eliminare	nu execută eliminările pe care le aprobă

– personalul primește cel puțin o dată la 12 luni instruire privind amenințările noi și practicile de securitate actuale, precum și privind practicile arhivistice și prezentul document, cu proces-verbal (secțiunea 6.12); la instruirea din ianuarie 2026 au participat 17 persoane, dintre care 4 operatori de arhivă electronică, între care un arhivar atestat, și 7 responsabili IT pentru arhivarea electronică.

20.4. Securitatea fizică

Infrastructura serviciului este găzduită în centrele de date ale CERTDIGITAL (secțiunea 14.1), cu controalele din Politicile generale (capitolul 8): acces fizic controlat pe zone de securitate, cu autentificare în mai mulți factori, sisteme de alarmă și de supraveghere video, intervenție de pază, alimentare de rezervă (UPS și, în centrul de date principal, generator) și două legături de Internet, la operatori diferiți.

20.5. Securitatea rețelei și gestionarea vulnerabilităților

– rețeaua este segmentată pe zone de securitate; firewall-urile redundante blochează toate protocoalele și accesele care nu sunt necesare serviciului, iar sistemele de detectare și prevenire a intruziunilor monitorizează traficul (secțiunea 6.14);

– administrarea se face numai din rețeaua internă dedicată (Politicile generale, secțiunea 9.5), cu autentificare cu cel puțin doi factori;

– componentele serviciului se autentifică reciproc, prin certificate, înainte de a comunica, iar certificatele TLS se validează la fiecare conexiune;

– vulnerabilitățile se scanează cel puțin o dată pe trimestru, iar testul de penetrare se face cel puțin o dată pe an și după schimbări semnificative; vulnerabilitățile se remediază în funcție de criticitate, cu retestare (Politicile generale, secțiunea 9.2).

20.6. Monitorizarea și disponibilitatea

– serviciul se monitorizează permanent: disponibilitatea interfețelor, capacitatea de stocare și cotele, replicarea, copiile de rezervă, verificările de integritate, augmentările, disponibilitatea serviciilor de marcare temporală și de păstrare și evenimentele de securitate; alertele se transmit personalului de serviciu;

– disponibilitatea-țintă este de cel puțin 99,5% pe an, cu excepția intervențiilor planificate, anunțate în prealabil pe site (secțiunea 6.13).

20.7. Continuitatea și recuperarea în caz de dezastru

– continuitatea serviciului se asigură conform Procedurii de continuitate operațională și de recuperare în caz de dezastru (PO_SI_63) și Planului de continuitate a afacerii (PO_C_SI_S_63); centrul de date secundar preia serviciul atunci când întreruperea estimată depășește RTO-ul serviciului (Politicile generale, capitolul 12);

– comutarea este controlată: se decide de echipa de management și acțiune în caz de urgență, convocată de Directorul General, și se execută de personalul cu roluri de încredere, conform procedurii;

– obiectivele de recuperare ale serviciului (RTO și RPO) sunt cele stabilite conform secțiunii 6.13; RPO-ul se asigură prin replicarea la cel mult 5 minute (secțiunea 14.2);

– înaintea reluării serviciului în centrul de date secundar sau după o restaurare din copiile de rezervă se verifică amprentele fișierelor arhivate față de registrul arhivei și de manifeste, lanțul jurnalului de audit și disponibilitatea cheii de sigiliu a serviciului, a serviciului de marcare temporală și a serviciului de păstrare calificată (secțiunea 13.7); după o restaurare din copii se reaplică eliminările aprobate după data copiei (secțiunea 18.4);

– depunerile primite în ultimul interval de replicare dinaintea întreruperii se reconciliază cu confirmările transmise; titularii dreptului de dispoziție ale căror depuneri confirmate nu se regăsesc în centrul de date secundar sunt informați, pentru a le depune din nou;

– dacă un eveniment afectează simultan ambele centre de date, arhiva se recuperează din copia offline (secțiunea 14.3), cu pierderea datelor ulterioare ultimei copii offline; abonații sunt informați, iar depunerile ulterioare acestei copii se reiau;

– comutarea efectivă în centrul de date secundar se testează cel puțin o dată pe an, cu proces-verbal care consemnează durata efectivă față de RTO și datele pierdute față de RPO, iar rezultatele testelor stau la baza actualizării procedurilor (ETSI EN 319 401, REQ-7.11.2-04X).

– compromiterea, suspiciunea de compromitere sau pierderea cheii private CERTDIGITAL QEARCH SERVICE G5 se tratează ca dezastru: sigilarea cu cheia afectată se oprește, iar operațiile care necesită sigiliul serviciului se pun în coadă până la restabilire (secțiunea 13.4); ofițerul de securitate IT stabilește momentul cunoscut al compromiterii și cere revocarea certificatului de sigiliu de către CERTDIGITAL QCA G5; ADR, abonații și părțile care se bazează se notifică conform secțiunii 20.9; cheia nouă se generează în ceremonie, sub control dual (secțiunea 20.1), iar serviciul se reia numai după emiterea și verificarea certificatului nou; rapoartele, manifestele și sigiliile periodice ale jurnalelor create după momentul compromiterii se emit din nou cu cheia nouă; la pierderea cheii fără compromitere, cheia se restaurează sub control dual dintr-o copie de rezervă (secțiunea 20.1) (ETSI EN 319 401, cl. 7.11).

Obiectivele de recuperare ale serviciului sunt RTO de 24 de ore și RPO de cel mult 5 minute pentru fișierele arhivate, bazele de date și jurnale.

20.8. Lanțul de aprovizionare

– CERTDIGITAL nu folosește subcontractanți pentru operarea serviciului (secțiunea 6.13); sistemul AE este dezvoltat de CENTRUL DE CALCUL S.A., iar codul lui sursă se depune la Arhivele Naționale, potrivit Legii nr. 135/2007, la fiecare schimbare semnificativă a sistemului (pentru versiunea din 2025, depunerea a fost confirmată de Serviciul Județean Gorj al Arhivelor Naționale la 06.06.2025);

– componentele terților (sistemul de operare, serverul de baze de date, cadrul de dezvoltare al aplicației, platforma de virtualizare și de stocare, modulele criptografice) se achiziționează conform procedurii de achiziții, cu evaluarea furnizorilor și cu obligații contractuale de securitate (CEN/TS 18170, cl. 7.15);

– actualizările se obțin numai din sursele oficiale ale producătorilor și se testează înainte de instalarea în producție (Politicile generale, secțiunea 9.1);

– serviciile de marcare temporală (serviciu calificat) și de păstrare (pentru care se solicită statutul calificat) folosite sunt servicii proprii ale CERTDIGITAL.

20.9. Gestionarea incidentelor

– incidentele se tratează conform procedurilor interne și se notifică conform Procedurii de notificare a incidentelor (00q): ADR, în cel mult 24 de ore de la luarea la cunoștință (art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS), DNSC, ANSPDCP, în cel mult 72 de ore, dacă sunt afectate date cu caracter personal, și persoanele afectate (secțiunea 6.13);

– pentru documentele arhivate, CERTDIGITAL, în calitate de persoană împuternicită, informează abonatul fără întârzieri nejustificate (art. 33 alin. (2) din Regulamentul (UE) 2016/679);

– sunt incidente specifice serviciului: neconcordanțele de integritate (secțiunea 13.7), eșecul reînnoirii dovezilor sau al augmentării (secțiunile 13.6 și 15.3), pierderea unei copii a arhivei, accesul neautorizat la documente și eliminarea eronată;

– după fiecare incident se analizează cauzele și se stabilesc măsuri de corectare, urmărite până la închidere.

20.10. Încetarea serviciului și transferul arhivelor

– încetarea se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530, și anexei acestuia pentru arhivarea electronică; planul se revizuiește cel puțin o dată la doi ani (secțiunea 6.15);

– ADR este informată cu cel puțin trei luni înainte de încetare, iar în cazul unei încetări neprevăzute, în cel mult 24 de ore; abonații sunt informați în termenele din plan, iar în cazul încetării anticipate, cu cel puțin 60 de zile înainte, cu identitatea succesorului propus și cu dreptul de a refuza transferul (secțiunea 6.15);

– abonații aleg între transferul arhivei, cu acordul lor, la un alt prestator de servicii de încredere calificat care prestează serviciul calificat de arhivare electronică, înscris cu acest serviciu într-o listă de încredere, și care, pentru arhivele supuse Legii nr. 135/2007, este și administrator de arhivă electronică acreditat de ADR (secțiunea 6.15), transferul arhivei la un alt prestator ales de abonat și restituirea arhivei prin export complet (secțiunea 16.4); se transferă sau se restituie AIP-urile, cu dovezile, rapoartele și jurnalele, împreună cu rapoartele de integritate și cu raportul de export sigilat; pentru profilul cu păstrare calificată, înainte de predare se aplică o ultimă augmentare a dovezilor (secțiunea 15.2);

– pentru arhivele administrate și potrivit Legii nr. 135/2007, transferul respectă și obligațiile din acest regim: ADR primește formularul de notificare a încetării activității de administrator al arhivei electronice, cu administratorul care preia arhivele și cu măsurile luate pentru abonați (art. 9 din procedura de acreditare a administratorilor de arhivă electronică și anexa nr. 1.3 la aceasta, aprobate prin Ordinul MCID nr. 20.717/2024), iar registrul arhivei electronice se predă odată cu arhivele;

– predarea se face pe baza exportului complet, al cărui index XML conține identificatorii persistenți și metadatele de regăsire ale fiecărui AIP, astfel încât documentele să poată fi regăsite la succesor; succesorul sau abonatul confirmă preluarea prin verificarea amprentelor din raportul de export, iar pentru fiecare abonat se întocmește un proces-verbal de predare (ISO 14721:2025, 3.3.6; CEN/TS 18170, cl. 12);

– documentele nu se elimină înainte de transfer sau de restituire; arhiva abonatului care nu își exprimă opțiunea în termenul comunicat nu se transferă: ea rămâne disponibilă pentru export și se păstrează, cu dovezile, de custodele înregistrărilor stabilit în planul de încetare; jurnalele și dovezile care nu se transferă se păstrează prin custode, pe durata rămasă.

20.11. Evaluarea conformității și auditul

– serviciul este evaluat de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162, în raport cu Regulamentul eIDAS, CEN/TS 18170 și anexa la Regulamentul de punere în aplicare (UE) 2025/2532, înaintea acordării statutului calificat și apoi cel puțin o dată la 24 de luni (secțiunea 6.16); atestarea de conformitate se publică în depozit;

– CERTDIGITAL efectuează anual un audit intern al serviciului;

– în regimul național, sistemul AE a fost auditat extern potrivit Ordinului MCID nr. 20.717/2024, în perioada februarie–mai 2025, cu opinie fără rezerve, și are avizul tehnic al ADR (secțiunea 4.2).

21. Aspecte juridice și comerciale

Tarifele, răspunderea, asigurarea, protecția datelor cu caracter personal, modificările, soluționarea litigiilor și legea aplicabilă sunt cele din capitolele 7 și 8 și din termenii și condițiile serviciului (TC-QEArch). Pe scurt:

– CERTDIGITAL răspunde conform art. 13 din Regulamentul eIDAS (secțiunea 7.4); limitările de utilizare se publică în termenii și condițiile serviciului;

– asigurarea de răspundere civilă profesională este cea de la secțiunea 7.5;

– pentru documentele arhivate, CERTDIGITAL este persoană împuternicită a abonatului (art. 28 din Regulamentul (UE) 2016/679), iar pentru datele de cont, jurnale și rapoarte este operator (secțiunea 8.2);

– abonatul păstrează toate drepturile asupra documentelor depuse (secțiunea 8.6);

– organismul de supraveghere este Autoritatea pentru Digitalizarea României (secțiunea 8.5);

– accesibilitatea serviciului pentru persoanele cu dizabilități se urmărește conform art. 15 din Regulamentul eIDAS (secțiunea 8.6).

Anexa A – Corespondența practicilor cu cerințele Regulamentului (UE) 2025/2532 și ale CEN/TS 18170

Cerință	Conținut	Politica (Partea I)	Practicile (Partea a II-a)
Regulamentul eIDAS, art. 45i alin. (2)	prezumția de integritate și de acuratețe a originii	1.1	13, 16.3
Regulamentul eIDAS, art. 45j alin. (1) lit. (a)	prestat de un prestator calificat; statut calificat	5.1	10, 20.11
Regulamentul eIDAS, art. 45j alin. (1) lit. (b)	durabilitate și lizibilitate dincolo de perioada de valabilitate tehnologică	6.5, 6.7	12.5, 13.6, 19
Regulamentul eIDAS, art. 45j alin. (1) lit. (c)	protecție împotriva pierderii și modificării; schimbări de suport sau de format	6.5, 6.7	13.7, 14, 19
Regulamentul eIDAS, art. 45j alin. (1) lit. (d)	raport automat de integritate, cu sigiliu calificat	6.9	13.3, 16.3
Regulamentul (UE) 2025/2532, art. 1	semnături și sigilii calificate; păstrare calificată	4.4, 6.6	15
Regulamentul (UE) 2025/2532, anexa, lit. (a)	referințe normative	2.1	10
Regulamentul (UE) 2025/2532, anexa, lit. (b) / CEN/TS 18170, cl. 6.1 / ETSI EN 319 401, cl. 5	politică și declarație de practici; publicare; notificări ADR (o lună / trei luni)	1.1, 6.1, 6.15, 8.3	10.1, 10.2, 20.10
Regulamentul (UE) 2025/2532, anexa, lit. (c) / CEN/TS 18170, cl. 6.2	termeni și condiții, publici și individuali, înainte de contract	6.2	11.1
Regulamentul (UE) 2025/2532, anexa, lit. (d) / CEN/TS 18170, cl. 7.3	personal; instruire la 12 luni	6.12	20.3
Regulamentul (UE) 2025/2532, anexa, lit. (e) / CEN/TS 18170, cl. 7.6	confidențialitate; originea prin semnături sau sigilii calificate; chei în dispozitive certificate; ECCG ACM; autentificare reciprocă	6.3, 6.5, 6.14	11.3, 11.5, 12.3, 14.4, 20.1, 20.2, 20.5
Regulamentul (UE) 2025/2532, anexa, lit. (f) / CEN/TS 18170, cl. 7.9 / ETSI EN 319 401, cl. 7.8	securitatea rețelei; scanare trimestrială; test de penetrare anual; firewall	6.14	20.5
Regulamentul (UE) 2025/2532, anexa, lit. (g) / CEN/TS 18170, cl. 7.11	colectarea dovezilor (evenimente critice și necritice)	6.11	17.4, 17.5
Regulamentul (UE) 2025/2532, anexa, lit. (h) / CEN/TS 18170, cl. 7.13	încetare; plan de încetare conform Regulamentului de punere în aplicare (UE) 2025/2530	6.15	20.10
Regulamentul (UE) 2025/2532, anexa, lit. (i) / CEN/TS 18170, cl. 13.3.1	timp de încredere; mărci temporale calificate	6.11	13.4
CEN/TS 18170, cl. 6.3–6.4	politica de securitate a informației; acordul de serviciu și acordul de depunere	6.2, 6.13	11.1, 20
CEN/TS 18170, cl. 7	organizare, active, control al accesului, securitate fizică, operare, vulnerabilități, incidente, continuitate, conformitate	6.13	17, 20
CEN/TS 18170, cl. 7.15	lanțul de aprovizionare; fără subcontractanți de operare	1.3, 6.13	20.8

Cerință	**Conținut**	**Politica (Partea I)**	**Practicile (Partea a II-a)**
CEN/TS 18170, cl. 8–9	pachetele de informații; SIP: formate, transmitere, primire, verificare	4.1, 6.3	11.4, 11.5, 12
CEN/TS 18170, cl. 10.2–10.4	AIP: generare, stocare, localizare, integritate	6.5	13.5, 13.7, 14
CEN/TS 18170, cl. 9.5, 10.2.5–10.2.6, 10.5	formatele admise; conversia formatelor; migrarea suporturilor	6.7	12.5, 19
CEN/TS 18170, cl. 10.6	eliminarea	6.10	18
CEN/TS 18170, cl. 11–12	DIP; transferul la alt prestator	6.8, 6.15	16, 20.10
CEN/TS 18170, cl. 13	trasabilitate; evenimente critice și necritice; protecția integrității	6.11	17.4, 17.5
CEN/TS 18170, cl. 14	rapoarte	6.4, 6.9, 6.10	12.7, 16.3, 18.5
ISO 14721:2025 (OAIS)	comunitatea desemnată și baza ei de cunoștințe; acordul de depunere; modelul informațional: SIP, AIP, DIP, AIU și AIC, informația de conținut, informațiile de reprezentare, PDI, informațiile de împachetare și descriptive; obiectivele de păstrare	3.1, 4.1, 5.2, 6.2–6.10	11.1, 12.2, 12.5, 13.1, 13.5, 16.2, 16.4, 19; anexa B
ETSI EN 319 401, cl. 7.10	jurnalizarea evenimentelor	6.11	17.4, 17.5
Legea nr. 135/2007 și Ordinul MCID nr. 20.717/2024	administrator de arhivă electronică; avizul sistemului și notificarea modificărilor lui; politica de conservare a documentelor pe termen lung; încetarea și transferul arhivelor	4.2, 4.5, 6.15	10, 20.10, 20.11

Anexa B – Corespondența cu modelul de referință OAIS (ISO 14721:2025)

Tabelul pune în corespondență termenii și componentele modelului de referință OAIS (ISO 14721:2025, 1.4 și 1.6.2) cu termenii și secțiunile prezentului document și cu elementele sistemului AE. Ultima coloană arată denumirea folosită în interfața web a sistemului AE, la punctul de acces al serviciului calificat (secțiunea 4.2), acolo unde există una; „—” arată că elementul nu are o denumire proprie în interfață.

Termenul OAIS	ISO 14721:2025	Corespondentul în prezentul document	Secțiunea	Sistemul AE (eArhivare)
comunitatea desemnată (Designated Community) și baza ei de cunoștințe (Knowledge Base)	1.6.2, 2.2, 3.2	abonații, titularii dreptului de dispoziție, utilizatorii și beneficiarii autorizați și părțile care se bazează; baza de cunoștințe: limba documentului, programele larg disponibile pentru formatele admise, un validator conform Regulamentului de punere în aplicare (UE) 2025/1945, nomenclatorul arhivistic și schema de metadate a tipului de document	5.2	—
producătorul (Producer)	2.2, 2.6.3	abonatul (depunătorul), utilizatorul care depune și titularul dreptului de dispoziție	1.3, 11.2	organizația; utilizatorii ei; titularul dreptului de dispoziție (TDD)
consumatorul (Consumer)	2.2, 2.6.4	utilizatorii autorizați, beneficiarii autorizați și părțile care se bazează	1.3, 16	utilizatorii cu drept de acces; „Solicitare acces la un document”
conducerea (Management)	2.2, 2.6.2	Directorul General, care aprobă prezentul document, în cadrul Politicilor generale CertDigital	1.5, 8.3	—
acordul de depunere (Submission Agreement)	1.6.2, 2.6.3	acordul de depunere din contract: formatele și metadatele pachetelor depuse, transmiterea, verificările la primire, codurile de răspuns și tratarea legăturilor către resurse externe	6.2, 11.1, 12	„Nomenclator arhivistic” (tipurile de documente, termenele de păstrare și schema de metadate); „Formate electronice”
acordul de comandă (Order Agreement)	1.6.2, 2.6.4	drepturile de acces aprobate de titularul dreptului de dispoziție și cererea de export, care stabilesc ce se livrează, în ce formă și pe ce cale	16.2, 16.4, 17.1	„Solicitare acces la un document” și „Solicitări către mine” (permisiunile, intervalul, accesul unic)
pachetul de informații depus (SIP)	2.3.4, 4.3.3.3	pachetul depus: documentul și fișa de însoțire	12.1, 12.2	„Adăugare document” (încărcarea și completarea fișei)

Termenul OAIS	ISO 14721:2025	Corespondentul în prezentul document	Secțiunea	Sistemul AE (eArhivare)
pachetul de informații arhivat (AIP)	2.3.4, 4.3.3.4	pachetul arhivat, cu componentele de la secțiunea 13.5	13.5	documentul arhivat din „Registru organizație”, cu fișa, „Evidențe prezervare” și „Istoric audit”
pachetul de informații livrat (DIP)	2.3.4, 4.4.5	pachetul livrat: documentul, metadatele, dovezile de arhivare și raportul de integritate; pachetul de export	16.2–16.4	„Descarcă” și „Exportă dovadă”, în detaliul documentului
unitatea de informații arhivate (Archival Information Unit, AIU)	1.6.2, 4.3.3.6	AIP-ul fiecărui document	13.5	documentul din registru, identificat prin GUID
colecția de informații arhivate (Archival Information Collection, AIC) și colecția de acces (Access Collection)	1.6.2, 4.3.3.8, 4.3.3.9	arhiva abonatului, cu PDI proprii (AIC); compartimentele, pachetele și dosarele din structura arhivei și grupele de acces (colecții de acces)	13.5	spațiul organizației; „Structura arhivei” (compartimente, pachete, dosare); „Grupe de acces”
informația de conținut (Content Information)	1.6.2, 4.3.2.4.2	obiectele depuse, exact cum au fost primite, cu informațiile lor de reprezentare, și versiunile rezultate din migrare	12.5, 13.5, 19.2	fișierul încărcat
informațiile de reprezentare (Representation Information): de structură, semantice și altele	2.3.2, 4.3.2.3	formatul identificat și versiunea lui, specificația din registrul formatelor, schema și descrierea câmpurilor (XML, CSV), limba documentului, schema de metadate a tipului de document	5.2, 12.2, 12.5, 13.5, 19.1	„Formate electronice”; schema de metadate a tipului de document din „Nomenclator arhivistic”
PDI – informațiile de referință (Reference Information)	4.3.2.4.3	identificatorul unic persistent al fiecărui obiect; identificatorii profilului și ai prezentului document	12.2, 12.7, 13.5	GUID; OID
PDI – informațiile de proveniență (Provenance Information)	4.3.2.4.3	depunătorul, emitentul și titularul dreptului de dispoziție; semnătura titularului și rezultatele validării; raportul de confirmare; istoricul AIP (verificări, reînnoiri, migrări, blocări legale); jurnalele	12.3, 13.2, 13.5, 17.4	fișa documentului („Părți și responsabilitate”, „Lanț de custodie”, semnăturile); „Istoric audit”
PDI – informațiile de context (Context Information)	4.3.2.4.3	tipul documentului; încadrarea în nomenclatorul arhivistic și în dosar; legăturile dintre original și versiunile migrate și cele cu documentele referite depuse separat	12.2, 13.5, 19.2	tipul documentului; dosarul; „Nomenclator arhivistic”
PDI – informațiile de fixitate (Fixity Information)	4.3.2.4.3	amprentele SHA-256; manifestul pachetului, sigilat și marcat temporal calificat; dovezile primite de la QPS	13.1, 13.5–13.7	amprenta SHA-256; „Evidențe prezervare”

Termenul OAIS	ISO 14721:2025	Corespondentul în prezentul document	Secțiunea	Sistemul AE (eArhivare)
PDI – informațiile privind drepturile de acces (Access Rights Information)	4.3.2.4.3	nivelul de clasificare, regimul de acces, drepturile acordate, perioada de păstrare și blocarea legală	12.2, 17.1, 18	„Nivel clasificare”; „Grupe de acces”; solicitările de acces; termenul de păstrare
informațiile de împachetare (Packaging Information)	4.3.2.4.4	manifestul pachetului arhivat, care enumeră componentele AIP și amprentele lor; indexul XML al pachetului de export	13.5, 16.4	—
informațiile descriptive (Descriptive Information)	4.3.2.4.5	metadatele fișei de însoțire (descrierea, cuvintele-cheie, tipul și datele documentului) și textul recunoscut optic, folosite la căutare	12.2, 16.1	fișa documentului; „Căutare avansată”; „Căutare OCR”
descrierea pachetului (Package Description): descrierea unității (Unit Description) și descrierea colecției (Collection Description)	4.3.3.5, 4.3.3.7, 4.3.3.9	înregistrarea fiecărui document în registrul arhivei; descrierea colecțiilor de acces	13.5, 16.1	rândul documentului din „Registru organizație”; listele din „Structura arhivei”
obiectivele de păstrare (Preservation Objectives)	1.6.2, 2.4	pentru formatele cu lizibilitate garantată, redarea documentului cu programe larg disponibile, cu conținutul și aspectul originalului; pentru celelalte formate, păstrarea nemodificată a fișierului; pentru profilul cu păstrare calificată, validarea semnăturilor și a sigiliilor calificate; pentru toate documentele, dovada integrității și a originii, prin raportul de integritate	4.3, 6.7, 12.5, 15, 16.3, 19.1	—
entitățile funcționale (Functional Entities)	4.2	depunerea (Ingest, capitolul 12); stocarea (Archival Storage, capitolul 14); registrul arhivei și metadatele (Data Management, capitolele 12 și 13); operarea (Administration, capitolele 17 și 20); monitorizarea formatelor și migrarea (Preservation Planning, capitolul 19); regăsirea și livrarea (Access, capitolul 16)	12–20	—

Precizări:

– „pachetul” din structura arhivei unui abonat în sistemul AE (compartiment, pachet, dosar) este o unitate de clasificare a documentelor, nu un pachet de informații (secțiunea 3.1);

– obiectivele PDS, PGD și AUG ale serviciului de păstrare calificată (PSPPS) sunt obiective de păstrare în sensul ETSI TS 119 511, nu obiectivele de păstrare din ISO 14721:2025, 2.4.