

Politica și declarația de practici a serviciului calificat de atestare electronică a atributelor

CertDigital QEAA

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, cu politicile atestatelor în anexa A) și declarația de practici (Partea a II-a) a serviciului calificat de atestare electronică a atributelor; Reg. (UE) 2025/1569 modificat prin 2026/1735; formatele din Reg. (UE) 2026/1731; 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	Completări pentru evaluarea conformității (ETSI TS 119 471): corespondența cu documentele prevăzute de standard (1.2); cerințele modificate prin RE 2026/1735 (2.1); controlul atestatului și excepțiile (6.3.1); nu se emit atestate de scurtă durată, toate atestatele pot fi revocate (6.7, 12.6); reînnoirea (12.5); riscul de corelare (13.2); informațiile predate la încetare (13.3); politicile atestatelor completate (anexa A); schema atributelor (anexa C, nouă); anexa B completată; generarea cheii	02/11/2026

		serviciului într-o ceremonie conformă procedurii de generare a cheilor (4.5)	
1.5	Ofițer de Securitate IT	Completări pentru evaluarea conformității (ETSI TS 119 471 și ETSI EN 319 401 V3.2.1, cu adaptările din RE (UE) 2026/1735): validarea datelor PID/LPID la orice emitere în portofel (12.2); nivelul ridicat al dispozitivului securizat al portofelului, dovada posesiei cheilor și revocarea imediată la suspendarea sau revocarea unității de portofel (11.3, anexa A); motivele de revocare și informarea solicitantului și a persoanei juridice din contractul-cadru (6.7, 12.6); certificatul de acces în metadatele emitentului (11.2); fluxurile de prezentare (4.3); justificarea valabilității maxime (anexa A); evenimentele de securitate jurnalizate, monitorizarea și alertarea (6.9); compromiterea cheii de sigiliu sau a sistemelor serviciului (6.11); configurația întărită (6.12); administrarea documentului (1.5); subsecțiunile noi 14.1–14.7 (securitatea rețelei, monitorizarea și jurnalizarea, incidentele și vulnerabilitățile, copiile de siguranță și continuitatea, lanțul de aprovizionare, verificarea configurației, organizațiile externe); identificatorul REQ-6.1-03 din ETSI EN 319 401 V3.2.1 (1.2)	02/11/2026
1.6	Ofițer de Securitate IT	Verificarea identității solicitantului (12.2): pentru metodele care folosesc procedurile de la certificate, trimiteri la regulamentele interne de identificare, cu versiunea în vigoare; identificarea o face numai CERTDIGITAL, fără parteneri	10/11/2026

Cuprins

PARTEA I – Politica serviciului 8
1. Introducere 8
1.1. Prezentare generală 8
1.2. Identificarea documentului și a politicilor 8
1.3. Participanții și furnizorii externi 10
1.4. Utilizarea serviciului și efectele juridice 10
1.5. Administrarea documentului 11
2. Referințe normative 12
2.1. Acte normative și standarde 12
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. Interfața cu portofelele europene pentru identitatea digitală 16
4.3. Formatele atestatelor 16
4.4. Politicile atestatelor 17
4.5. Identitatea serviciului și sigiliul serviciului 17
5. Politica serviciului 18
5.1. Identificare și conformitate 18
5.2. Comunitatea utilizatorilor și aplicabilitatea 18
5.3. Modificarea politicii 18
6. Cerințele privind practicile 19
6.1. Publicare și depozit 19
6.2. Termeni și condiții 19
6.3. Cererea de emitere 19
6.3.1. Controlul atestatului 19
6.4. Verificarea identității 20
6.5. Verificarea atributelor 20
6.6. Emiterea atestatului 20

6.7. Valabilitatea, starea și revocarea 21
6.8. Separarea serviciului și protecția vieții private 22
6.9. Timpul de încredere și jurnalele 22
6.10. Personalul 23
6.11. Controale privind facilitățile, managementul și operarea 23
6.12. Controale criptografice și de rețea 24
6.13. Notificări către ADR și încetarea serviciului 24
6.14. Evaluarea conformității 24
7. Obligații și răspundere 25
7.1. Obligațiile CERTDIGITAL 25
7.2. Obligațiile solicitantului, ale subiectului și ale titularului 25
7.3. Obligațiile părților care se bazează 25
7.4. Răspunderea 25
7.5. Asigurarea 26
8. Alte aspecte comerciale și juridice 27
8.1. Tarife 27
8.2. Protecția datelor cu caracter personal 27
8.3. Modificări 27
8.4. Soluționarea litigiilor 27
8.5. Legea aplicabilă și cadrul legal 27
8.6. Alte prevederi 28
9. Corespondența cu cerințele Regulamentului eIDAS și ale regulamentelor de punere în aplicare ..29
9.1. Tabel de corespondență 29
PARTEA A II-A – Declarația de practici 31
10. Publicare și depozit 31
11. Interfața cu portofelele 32
11.1. Fluxul de emitere 32
11.2. Autentificarea reciprocă și înregistrarea 32
11.3. Validarea unității de portofel 32
11.4. Limite 33
12. Ciclul de viață al atestatului 34
12.1. Cererea 34
12.2. Verificarea identității 34

12.3. Verificarea atributelor 35
12.4. Emiterea și conținutul atestatului 35
12.5. Legarea de titular, loturile, reemiterea și reînnoirea 36
12.6. Revocarea și informațiile de stare 36
13. Datele, separarea și păstrarea 38
13.1. Separarea serviciului (art. 45h) 38
13.2. Riscul de corelare 38
13.3. Durata păstrării 38
13.4. Protecția datelor 39
14. Controale de management și operare 40
14.1. Securitatea rețelei 41
14.2. Monitorizarea și jurnalizarea 42
14.3. Incidentele și vulnerabilitățile 43
14.4. Copiile de siguranță și continuitatea 45
14.5. Lanțul de aprovizionare 46
14.6. Verificarea configurației 48
14.7. Organizațiile externe care susțin serviciul 49
15. Aspecte juridice și comerciale 50
Anexa A – Politicile atestatelor 51
A.1. Reprezentantul legal al persoanei juridice (OID 1.3.6.1.4.1.47898.15.1.1) 51
A.2. Datele de identificare ale persoanei juridice (OID 1.3.6.1.4.1.47898.15.1.2) 52
Anexa B – Corespondența practicilor (Partea a II-a) cu cerințele 53
Anexa C – Schema atributelor 54
C.1. Reprezentantul legal al persoanei juridice (A.1) 54
C.2. Datele de identificare ale persoanei juridice (A.2) 55

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 atestare electronică a atributelor**, adică la emiterea de **atestate electronice calificate ale atributelor** (art. 3 pct. 45, art. 24, 45b, 45d, 45e, 45g și 45h și anexa V din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183), și descrie practicile prin care CERTDIGITAL le îndeplinește.

Un atestat electronic calificat al atributelor confirmă, într-o formă electronică sigilată de CERTDIGITAL, unul sau mai multe atribute ale unei persoane fizice sau juridice (de exemplu, calitatea de reprezentant legal al unei societăți), verificate la emitere în raport cu sursa lor. Atestatele se emit, la cererea utilizatorului, în **portofelele europene pentru identitatea digitală** (art. 45g), în formatele SD-JWT VC și ISO/IEC 18013-5 (mdoc), și au același efect juridic ca atestatele emise în mod legal în format tipărit (art. 45b alin. (2)).

Serviciul face parte din generația G5 a infrastructurii CertDigital. Pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României cu tipul `EAA/Q`; până la înscriere, serviciul nu se prestează ca serviciu de încredere calificat (art. 21 alin. (3) din Regulamentul eIDAS).

Documentul are două părți. Partea I, politica serviciului, stabilește **ce** garantează CERTDIGITAL, pentru serviciu în ansamblu și, în anexa A, pentru fiecare tip de atestat (politica atestatului). **Cum** sunt îndeplinite cerințele este descris în Partea a II-a, declarația de practici a serviciului; corespondența practicilor cu cerințele este în anexa B, iar schema atributelor fiecărui tip de atestat este în anexa C. Pentru cerințele comune tuturor serviciilor se aplică Politicile generale CertDigital (PG).

1.2. Identificarea documentului și a politicilor

Element	Valoare
Titlu	Politica și declarația de practici a serviciului calificat de atestare electronică a atributelor CertDigital (PDP-QEAA)
Titlu în limba engleză	CertDigital Qualified Electronic Attestation of Attributes Service Policy and Practice Statement
Versiune	1.6
Data	10.11.2026
Identificator (OID)	1.3.6.1.4.1.47898.15.1 – prezentul document (politica serviciului și declarația de practici)

Element	Valoare
Politicile atestatelor	1.3.6.1.4.1.47898.15.1.1 – politica atestatului „Reprezentantul legal al persoanei juridice” (anexa A.1); 1.3.6.1.4.1.47898.15.1.2 – politica atestatului „Datele de identificare ale persoanei juridice” (anexa A.2)
Declarația de practici	declarația de practici este inclusă în prezentul document (Partea a II-a); identificatorul 1.3.6.1.4.1.47898.15.2, alocat inițial declarației de practici, nu se mai folosește
Cerințele ETSI respectate	ETSI TS 119 471 V1.1.1 (2025-05), cu adaptările din anexa I la Regulamentul de punere în aplicare (UE) 2025/1569, astfel cum a fost modificat prin Regulamentul de punere în aplicare (UE) 2026/1735; ETSI nu definește un identificator de politică pentru atestatele calificate, de aceea politica are numai identificatorul CertDigital
Specificații de referință	RE (UE) 2025/1569, modificat prin RE (UE) 2026/1735 (prestatorul: TS 119 471 V1.1.1 adaptat; atestatele: anexa II la RE (UE) 2024/2979, modificată prin RE (UE) 2026/1731, adică ETSI TS 119 472-1 V1.2.1, clauzele 2–6); RE (UE) 2024/2982, modificat prin RE (UE) 2026/1731 (emiterea în portofel: ETSI TS 119 472-3 V1.1.1)
Tipul de serviciu (ETSI TS 119 612)	`http://uri.etsi.org/TrstSvc/Svctype/EAA/Q`
Identitatea serviciului în Lista de încredere (după înscriere)	CERTDIGITAL QEAA SERVICE G5 (secțiunea 4.5)
Punctul de acces	interfața de emitere pentru portofele (secțiunile 4.2 și 11), la https://eaa.certdigital.ro (identificatorul emitentului OpenID4VCI; metadatele: https://eaa.certdigital.ro/.well-known/openid-credential-issuer)
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-qeaa_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Identificatorii sunt înscriși în CERTDIGITAL_OID_MAP. Certificatul de sigiliu QEAA G5 conține identificatorul politicii (1.3.6.1.4.1.47898.15.1), care identifică și prezentul document; identificatorul politicii fiecărui atestat se înscrie în descrierea publicată a tipului de atestat (secțiunea 6.1).

Corespondența cu documentele prevăzute de ETSI TS 119 471. Prezentul document cuprinde politica serviciului, declarația de practici a serviciului și politicile atestatelor, astfel:

Documentul prevăzut de ETSI TS 119 471	Partea din prezentul document
politica serviciului (EAA Service Policy, clauza 3.1)	Partea I (capitolele 1–9), cu identificatorul 1.3.6.1.4.1.47898.15.1
declarația de practici a serviciului (EAAS Practice Statement, clauza 6.1)	Partea a II-a (capitolele 10–15)
politicile atestatelor (EAA Policy, clauza 6.4), câte una pentru fiecare tip de atestat	anexa A: A.1, cu identificatorul 1.3.6.1.4.1.47898.15.1.1, și A.2, cu identificatorul 1.3.6.1.4.1.47898.15.1.2; schema atributelor în anexa C
termenii și condițiile (clauza 6.2)	document separat: Termenii și condițiile serviciului calificat de atestare electronică a atributelor (TC-QEAA)

Cerințele din ETSI EN 319 401, clauza 6.1, se aplică prin ETSI TS 119 471, REQ-EAASP-6.1.1-01. ETSI EN 319 401 V3.2.1 nu impune structura declarației de practici (REQ-6.1-03, nota 1), iar ETSI TS 119 471, clauza 6.4, admite includerea politicilor atestatelor în alte documente ale serviciului.

1.3. Participanții și furnizorii externi

– **prestatorul**: CERTDIGITAL, care verifică identitatea și atributele, emite și sigilează atestatele, gestionează starea lor și răspunde în ansamblu de serviciu;

– **solicitantul**: utilizatorul portofelului european pentru identitatea digitală care cere emiterea atestatului;

– **subiectul atestatului**: persoana fizică sau juridică la care se referă atributele atestate (anexa V lit. (c)); poate fi chiar solicitantul sau o persoană juridică pe care solicitantul o reprezintă;

– **titularul**: persoana în al cărei portofel se stochează atestatul și care îl prezintă părților care se bazează;

– **sursele autentice**: registrele publice sau private recunoscute ca surse primare ale atributelor (art. 3 pct. 47), de exemplu registrul comerțului ținut de Oficiul Național al Registrului Comerțului (ONRC), precum și mecanismul național de verificare a atributelor (art. 45e și art. 9 din RE 2025/1569), după punerea lui în funcțiune; sursele autentice se folosesc numai pentru verificarea atributelor, la cererea utilizatorului;

– **furnizorii de portofele**: furnizorii portofelelor europene pentru identitatea digitală (art. 5a), ale căror unități de portofel sunt verificate la emitere; listele de încredere ale furnizorilor de portofele se folosesc pentru validarea unităților de portofel;

– **organismul de înregistrare a părților care se bazează pe portofel** și **autoritatea care emite certificatele de acces** (RE 2025/848, modificat prin RE 2026/1730);

– **autoritatea de certificare CERTDIGITAL QCA G5**, care emite certificatul calificat de sigiliu al serviciului;

– **părțile care se bazează** pe atestate.

CERTDIGITAL nu deleagă către terți emiterea atestatelor, verificarea atributelor sau gestionarea cheilor serviciului.

1.4. Utilizarea serviciului și efectele juridice

– atestatul electronic calificat al atributelor are **același efect juridic ca atestatele emise în mod legal în format tipărit** (art. 45b alin. (2)) și nu face obiectul niciunei cerințe obligatorii în plus față de anexa V (art. 45d alin. (3));

– atestatul confirmă atributele așa cum figurau în sursa autentică la momentul verificării; el nu atestă alte fapte și nu suplinește documentele cerute de lege pentru acte juridice determinate;

– când identificarea electronică este obligatorie pentru accesarea unui serviciu public online, datele de identificare din atestat nu înlocuiesc mijlocul de identificare electronică, cu excepția cazului în care statul membru permite expres acest lucru (art. 45c);

– atestatele se folosesc numai pe durata lor de valabilitate și numai cât timp nu sunt revocate.

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; Compartimentul Servicii Electronice răspunde de menținerea documentului și pregătește reviziile, Directorul Tehnic evaluează dacă o modificare trebuie notificată ADR (Procedura de notificare, 00q, cap. 12), iar reviziile se consemnează în istoricul documentului. Documentul se revizuiește cel puțin anual și la orice schimbare a serviciului. 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. 44–47, art. 13, 15, 20, 21, 24, 45b–45h și anexele V și VI;

– Regulamentul de punere în aplicare (UE) 2025/1569 (atestatele electronice calificate ale atributelor), modificat prin Regulamentul de punere în aplicare (UE) 2026/1735 (aplicabil din 11.08.2026; modificările art. 9 se aplică din 01.01.2027);

– Regulamentul de punere în aplicare (UE) 2024/2979 (integritatea și funcționalitățile de bază ale portofelelor), anexa II, și Regulamentul de punere în aplicare (UE) 2024/2982 (protocoalele și interfețele portofelelor), ambele modificate prin Regulamentul de punere în aplicare (UE) 2026/1731;

– Regulamentul de punere în aplicare (UE) 2025/1566 (verificarea identității și a atributelor persoanelor cărora li se emit certificate calificate sau atestate calificate ale atributelor), aplicabil din 19.08.2027;

– Regulamentul de punere în aplicare (UE) 2025/848 (înregistrarea părților care se bazează pe portofel), modificat prin Regulamentul de punere în aplicare (UE) 2026/1730;

– Regulamentul de punere în aplicare (UE) 2025/2530 (cerințe pentru prestatorii calificați: notificări, gestionarea riscurilor, planul de încetare); Regulamentul de punere în aplicare (UE) 2025/2162 (acreditarea organismelor de evaluare a conformității);

– ETSI TS 119 471 V1.1.1 (cerințe de politică și securitate pentru prestatorii de servicii de atestare electronică a atributelor), cu adaptările din RE 2026/1735, inclusiv ETSI EN 319 401 V3.2.1 (2026-01) ca referință normativă;

– ETSI TS 119 472-1 V1.2.1 (profilurile atestatelor: SD-JWT VC, clauza 5, și mdoc, clauza 6), cu adaptările din RE 2026/1731; ETSI TS 119 472-3 V1.1.1 (profilul de emitere, OpenID for Verifiable Credential Issuance); ETSI TS 119 472-2 (prezentarea atestatelor, informativ pentru prestator);

– ETSI TS 119 412-6 V1.1.1, clauza 7, ETSI EN 319 412-1 și ETSI EN 319 412-3 (profilul certificatului de sigiliu al serviciului);

– ETSI TS 119 461 V2.1.1 (verificarea identității), aplicabil prin RE 2025/1566; ETSI TS 119 478 V1.1.1 (interfețele cu sursele autentice);

– IETF SD-JWT VC; IETF Token Status List (draft-ietf-oauth-status-list-20); ISO/IEC 18013-5; OpenID for Verifiable Credential Issuance 1.0;

– documentul „Agreed Cryptographic Mechanisms” al ECCG, publicat de ENISA; schema EUCC (RE 2024/482 și 2024/3144); FIPS PUB 140-3;

– Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026; Regulamentul (UE) 2016/679 și Legea nr. 190/2018; Legea nr. 242/2022 (Platforma națională de interoperabilitate).

Cerințele ETSI TS 119 471 citate cu identificatorii REQ-EAASP-4.2.2.3-02, 4.2.2.3-03, 6.1-02, 6.3-02, 7.5.3-01A, 7.5.3-01B, 7.5.3-02, 7.9-02 și 7.12-04 au textul stabilit sau modificat prin anexa I la Regulamentul de punere în aplicare (UE) 2026/1735; cerința REQ-EAASP-6.1-02 are, prin această anexă, nivelul obligatoriu („shall”). Clauzele 4.2.2.2 și 4.3.2 din ETSI TS 119 471 nu se aplică. Identificatorii se citează în forma normalizată: REQ-EAASP-4.2.2.1-09 (scris în standard „REQ-EAASP-4.2.2.1.09”); cerința privind reînnoirea se citează cu prefixul din standard, REQ-EAAS-4.2.4.1-01; trimiterea din REQ-EAASP-4.2.5.2-06 la „REQ-EAASP-4.2.5-05”, care nu există în standard, se citește ca trimitere la REQ-EAASP-4.2.5.1-04.

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

3. Definiții și acronime

3.1. Definiții

– **atestat electronic al atributelor** — atestat în format electronic care permite autentificarea atributelor (art. 3 pct. 44 din Regulamentul eIDAS);

– **atestat electronic calificat al atributelor** — atestat electronic al atributelor emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele din anexa V (art. 3 pct. 45);

– **sursă autentică** — registru public sau privat, considerat sursa primară a unor informații sau atribute (art. 3 pct. 47);

– **politica atestatului** — setul de reguli aplicabile unui tip de atestat: atributele, sursa și metoda de verificare, formatul, valabilitatea și starea (ETSI TS 119 471);

– **sistem de atestare** — schema unui tip de atestat, înregistrată în catalogul sistemelor de atestare a atributelor (art. 3 alin. (2) din RE 2025/1569);

– **atestat de scurtă durată** — atestat cu perioada de valabilitate mai mică de 24 de ore, din care prestatorul poate omite informațiile de revocare, dacă declarația de practici o prevede expres (ETSI TS 119 471, REQ-EAASP-4.2.5.2-06); CERTDIGITAL nu emite atestate de scurtă durată (secțiunea 12.6);

– **lista de stare** — structura publicată de CERTDIGITAL, sigilată, din care o parte care se bazează află dacă un atestat este sau nu revocat (IETF Token Status List);

– **legarea de titular** — legarea criptografică a atestatului de o cheie a portofelului titularului, a cărei posesie se dovedește la prezentare;

– **divulgare selectivă** — posibilitatea titularului de a prezenta numai o parte din atributele atestate.

3.2. Acronime

Acronim	Semnificație
CAB	organism de evaluare a conformității (conformity assessment body)
COSE	formatul de semnătură CBOR Object Signing and Encryption, folosit de atestatele mdoc
CWT	token CBOR Web Token
EAA	atestat electronic al atributelor (electronic attestation of attributes)
EAAP	politica atestatului (electronic attestation of attributes policy)
JWS	semnătură JSON Web Signature
JWT	token JSON Web Token
mdoc	atestat în formatul ISO/IEC 18013-5
MSO	obiectul de securitate al atestatului mdoc (mobile security object)
OpenID4VCI	protocolul OpenID for Verifiable Credential Issuance
PID	datele de identificare personală din portofel

Acronim	Semnificație
QEAA	atestat electronic calificat al atributelor
SD-JWT VC	atestat în formatul IETF SD-JWT VC
WUA	atestatul unității de portofel (wallet unit attestation)

4. Concepte generale

4.1. Serviciul și componentele sale

– **cererea**: solicitantul cere emiterea atestatului din portofelul său, prin interfața de emitere a CERTDIGITAL (secțiunea 4.2);

– **verificarea identității** solicitantului și a subiectului (art. 24 alin. (1a); secțiunea 6.4);

– **verificarea atributelor** în raport cu sursa autentică, prin metodele permise de art. 24 alin. (1b) (secțiunea 6.5);

– **emiterea**: întocmirea atestatului conform politicii lui (anexa A), sigilarea cu sigiliul electronic calificat al CERTDIGITAL și livrarea în portofel, legat de cheia titularului (secțiunea 6.6);

– **gestionarea stării**: publicarea listelor de stare și revocarea (secțiunea 6.7).

4.2. Interfața cu portofelele europene pentru identitatea digitală

CERTDIGITAL pune la dispoziție o interfață cu portofelele europene pentru identitatea digitală (art. 45g alin. (2)), prin care orice utilizator poate solicita, obține și stoca atestatele, indiferent de statul membru care a furnizat portofelul (art. 45g alin. (1)):

– emiterea folosește protocolul OpenID for Verifiable Credential Issuance, conform ETSI TS 119 472-3 V1.1.1; metadatele emitentului se publică la punctul de acces al serviciului;

– CERTDIGITAL se autentifică față de unitatea de portofel prin autentificare reciprocă, cu un certificat de acces valabil (REQ-EAASP-4.2.2.3-02), și validează unitatea de portofel, inclusiv faptul că nu a fost revocată (REQ-EAASP-4.2.2.3-03);

– CERTDIGITAL se înregistrează ca parte care se bazează pe portofel, cu dreptul de furnizor de atestate calificate, conform RE 2025/848, modificat prin RE 2026/1730.

4.3. Formatele atestatelor

Atestatele se emit în formatele din clauzele 2–6 ale ETSI TS 119 472-1 V1.2.1 (anexa II la RE 2024/2979, modificată prin RE 2026/1731): **SD-JWT VC** (clauza 5) și **mdoc** (ISO/IEC 18013-5, clauza 6). Formatele W3C Verifiable Credentials și certificatele de atribute X.509 nu se folosesc pentru atestatele calificate. Fiecare tip de atestat din anexa A se emite în ambele formate; formatul unei emiteri se stabilește în cererea de emitere, după formatele acceptate de portofel. Schema atributelor, pentru ambele formate, este în anexa C. Atestatele emise pot fi prezentate atât în fluxurile de proximitate (supravegheate și nesupravegheate), cât și în fluxurile la distanță (pe același dispozitiv și între dispozitive): formatul mdoc se prezintă în proximitate, conform ISO/IEC 18013-5, și la distanță, iar formatul SD-JWT VC la distanță; CERTDIGITAL nu restrânge fluxul de prezentare (ETSI TS 119 471, REQ-EAASP-4.2.2.3-14, REQ-EAASP-4.2.3.2-01).

4.4. Politicile atestatelor

Fiecare tip de atestat are o politică proprie, cu identificator, care stabilește: atributele și domeniul lor de aplicare, sistemul de atestare, subiectul și titularul, sursa autentică și metoda de verificare, formatele, valabilitatea maximă, regimul stării și cazurile specifice de revocare. Politicile în vigoare sunt cele din anexa A:

Politica atestatului	Subiectul	Atributele (anexa VI)	Sursa
Reprezentantul legal al persoanei juridice (47898.15.1.1)	persoana fizică înscrisă ca reprezentant legal	pct. 9 – împuterniciri și mandate de reprezentare	registrul comerțului (ONRC)
Datele de identificare ale persoanei juridice (47898.15.1.2)	persoana juridică	pct. 11 – date privind societățile	registrul comerțului (ONRC)

Un tip nou de atestat se introduce numai printr-o politică nouă, cu identificator propriu, publicată înainte de prima emitere.

4.5. Identitatea serviciului și sigiliul serviciului

Atestatele poartă **sigiliul electronic calificat al CERTDIGITAL** (anexa V lit. (g)), creat cu certificatul calificat de sigiliu dedicat serviciului, CERTDIGITAL QEAA SERVICE G5, care va identifica serviciul în Lista de încredere, după înscriere:

– profilul certificatului respectă ETSI TS 119 412-6 V1.1.1, clauza 7, și ETSI EN 319 412-3, cu politica QCP-l-qscd; certificatul conține numele CENTRUL DE CALCUL S.A., statul (RO) și identificatorul VATRO-2163993;

– cheia privată se generează, se păstrează și se utilizează numai într-un dispozitiv calificat de creare a sigiliului (REQ-EAASP-7.5.3-02; secțiunea 6.12) și se folosește numai pentru atestate și pentru informațiile de stare;

– certificatul este disponibil gratuit, la adresa indicată în fiecare atestat (anexa V lit. (h)).

Certificatul serviciului este CERTDIGITAL QEAA SERVICE G5, emis de CERTDIGITAL QCA G5, valabil 5 ani, cu cheie ECDSA P-256. Perechea de chei se generează în partiția SVG5 a modulelor Thales Luna PCIe HSM 7, într-o ceremonie desfășurată conform Procedurii privind generarea cheilor (document intern; REQ-EAASP-7.5.2-07), de personal numit în roluri de încredere, sub control dual, în prezența unui martor independent și cu înregistrare video, consemnată într-un raport care conține elementele prevăzute la REQ-EAASP-7.5.2-08 și 7.5.2-09 (secțiunea 14). Profilul certificatului este descris în DPC CERTDIGITAL G5, secțiunea 7.1.2, iar certificatul se publică la http://certs.certdigital.ro/certdigital_qeaa_g5.crt înainte de emiterea primului atestat.

5. Politica serviciului

5.1. Identificare și conformitate

CERTDIGITAL declară conformitatea serviciului cu standardele și specificațiile din anexele I și II la RE 2025/1569, astfel cum a fost modificat prin RE 2026/1735. Conformitatea atestatelor cu anexa V se evaluează conform acestor standarde și specificații (art. 45d alin. (2)). Politicile și procedurile prin care CERTDIGITAL respectă cerințele sistemelor de atestare înregistrate în catalog fac parte din evaluarea conformității (art. 3 alin. (2) din RE 2025/1569). Pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere (art. 21); 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 care trebuie să dovedească atribute în relația cu autorități și instituții publice, instituții financiare, profesioniști și alte părți care se bazează, în România și în celelalte state membre.

5.3. Modificarea politicii

Dacă o modificare a prezentului document sau a politicii unui atestat afectează garanțiile oferite, identificatorul politicii respective se schimbă. O modificare a practicilor din Partea a II-a care nu afectează garanțiile se face printr-o versiune nouă a documentului, cu același identificator. Atestatele emise anterior rămân guvernate de politica în vigoare la data emiterii lor.

6. Cerințele privind practicile

6.1. Publicare și depozit

La https://www.certdigital.ro/repository/ se publică, 24/7, public și fără restricții de acces: prezentul document, cu politicile atestatelor (anexa A), termenii și condițiile serviciului, descrierea tipurilor de atestat (inclusiv identificatorii tipurilor și sistemele de atestare), certificatele serviciului și adresele listelor de stare.

6.2. Termeni și condiții

Înainte de emitere, solicitantul este informat, clar, complet și ușor accesibil, despre termenii și condițiile serviciului: tipurile de atestat, atributele și sursele lor, valabilitatea, revocarea, obligațiile titularului, limitările de utilizare (inclusiv art. 45c), prelucrarea datelor, tarifele și răspunderea. Acceptarea termenilor și condițiilor de către solicitant se înregistrează.

6.3. Cererea de emitere

– atestatele se emit numai la cererea utilizatorului, pentru tipurile de atestat publicate;

– cererea se face din portofelul european pentru identitatea digitală, prin interfața de la secțiunea 4.2; CERTDIGITAL verifică dacă cererea este completă și stabilește subiectul atestatului;

– dacă solicitantul cere un atestat privind o altă persoană (de exemplu, persoana juridică pe care o reprezintă), CERTDIGITAL verifică și dreptul lui de reprezentare.

6.3.1. Controlul atestatului

Atestatul se emite în portofelul subiectului și se află sub controlul lui exclusiv (ETSI TS 119 471, REQ-EAASP-4.2.3.1-02). CERTDIGITAL nu emite atestatul în portofelul altei persoane și nu pune atestatul sau cheile de legare la dispoziția abonatului care acționează în numele subiectului, cu excepțiile de mai jos, stabilite de prezenta politică:

a) atestatul A.2, al cărui subiect este persoana juridică, se emite în portofelul persoanei juridice sau în portofelul reprezentantului ei legal, verificat conform anexei A.1; reprezentantul legal deține atestatul și îl prezintă numai în numele persoanei juridice;

b) când o persoană juridică solicită atestate prin contractul-cadru (CTR-QEAA), atestatele A.1 se emit numai în portofelul reprezentantului legal care este subiectul lor, la cererea acestuia, iar atestatele A.2 se emit numai în portofelul persoanei juridice sau al reprezentanților legali desemnați în anexa 2 la contract; persoana juridică nu primește atestatele A.1 și nici cheile de legare ale reprezentanților.

În ambele cazuri, persoana juridică poate cere oricând revocarea atestatelor A.2 al căror subiect este și a atestatelor A.1 emise reprezentanților ei, iar încetarea calității de reprezentant legal în registrul comerțului duce la revocarea atestatelor A.1 și A.2 deținute de acesta (anexa A).

6.4. Verificarea identității

– identitatea solicitantului și, după caz, a subiectului se verifică prin una dintre metodele de la art. 24 alin. (1a): (a) portofelul european pentru identitatea digitală sau un mijloc de identificare electronică notificat, cu nivel de asigurare ridicat; (b) un certificat calificat, o semnătură electronică calificată sau un sigiliu electronic calificat emise în condițiile lit. (a), (c) sau (d); (c) alte metode de identificare de încredere ridicată, confirmate de un organism de evaluare a conformității, precum identificarea la distanță CERTDIGITAL KYC; (d) prezența fizică;

– de la 19.08.2027, verificarea identității respectă ETSI TS 119 461 V2.1.1, cu adaptările din RE 2025/1566;

– metoda folosită, dovezile și momentul verificării se înregistrează.

6.5. Verificarea atributelor

– atestatul conține **numai atribute verificate la emitere**; politica fiecărui atestat stabilește sursa autentică și metoda de verificare dintre cele de la art. 24 alin. (1b);

– atributele se verifică electronic, în raport cu sursa autentică (de exemplu, datele registrului comerțului furnizate electronic de ONRC), iar CERTDIGITAL verifică autenticitatea și originea informațiilor primite;

– după ce România pune la dispoziție mecanismul de verificare prevăzut la art. 45e și la art. 9 din RE 2025/1569, atributele din anexa VI care se bazează pe surse autentice din sectorul public se verifică prin acest mecanism;

– sursa, metoda, momentul și rezultatul verificării se înregistrează pentru fiecare atribut și se păstrează ca dovadă.

CERTDIGITAL obține datele ONRC prin serviciile online ale ONRC, cu un cont de utilizator autentificat (e-mail, parolă și cod de validare transmis pe e-mail); integrarea automată prin serviciile expuse de ONRC este planificată.

6.6. Emiterea atestatului

CERTDIGITAL emite fiecare atestat în conformitate cu prezenta politică (Partea I) și cu politica atestatului din anexa A față de care declară conformitatea; identificatorul politicii atestatului este indicat în descrierea publicată a tipului de atestat (ETSI TS 119 471, REQ-EAASP-4.2.2.1-09).

– atestatul conține elementele din anexa V, în structurile din ETSI TS 119 472-1 (corespondența este în secțiunea 12.4): (a) mențiunea, prelucrabilă automat, că este atestat calificat (categoria `urn:etsi:esi:eaa:eu:qualified`); (b) statul (RO), denumirea și identificatorul CENTRUL DE CALCUL S.A.; (c) subiectul; (d) atributele și domeniul lor de aplicare; (e) începutul și sfârșitul valabilității; (f) un identificator unic și sistemul de atestare, dacă este

cazul; (g) sigiliul electronic calificat al CERTDIGITAL; (h) adresa certificatului de sigiliu; (i) informațiile despre starea certificatului de sigiliu, precum și adresa listei de stare și poziția atestatului în listă, prezente în toate atestatele, deoarece toate atestatele sunt supuse revocării (secțiunea 6.7);

– CERTDIGITAL nu folosește pseudonime în atestate;

– valabilitatea începe cel mai devreme la momentul emiterii, fără antedatare, și nu depășește valabilitatea maximă din politica atestatului;

– atestatul se leagă criptografic de o cheie a unității de portofel a titularului, a cărei posesie se verifică la emitere; legarea de portofel este obligatorie pentru toate tipurile de atestat (anexa A; ETSI TS 119 471, REQ-EAASP-4.2.2.3-06); atestatele se pot emite în loturi, cu chei și poziții în lista de stare distincte, pentru a împiedica corelarea prezentărilor;

– fiecare atribut se poate divulga selectiv; atestatul conține numai atributele necesare scopului său.

6.7. Valabilitatea, starea și revocarea

– **CERTDIGITAL nu emite atestate de scurtă durată**: toate atestatele conțin informații de stare și pot fi revocate atât la cerere, cât și din inițiativa CERTDIGITAL (secțiunea 12.6);

– **toate atestatele** au informații de stare publicate prin liste de stare (IETF Token Status List), cu numai două valori: nerevocat și revocat; **nu există suspendare**;

– revocarea este **definitivă**: atestatul își pierde valabilitatea din momentul revocării și nu poate reveni la statutul anterior (art. 45d alin. (4));

– numai CERTDIGITAL poate revoca atestatele pe care le emite (art. 4 alin. (2) din RE 2025/1569). Revocarea are loc cel puțin: (a) la cererea persoanei pentru care s-a emis atestatul sau a subiectului; (b) când CERTDIGITAL ia cunoștință de compromiterea securității sau a credibilității atestatului; (c) în alte situații prevăzute de dreptul Uniunii sau de dreptul intern (art. 4 alin. (3)). Revocarea are loc și în următoarele situații: atributul nu mai corespunde sursei autentice; datele furnizate s-au dovedit false; atestatul a fost emis cu o eroare; atestatul nu mai este conform cu prezentul document (politica serviciului sau declarația de practici) ori cu politica atestatului sub care a fost emis; CERTDIGITAL ia cunoștință de orice altă modificare care afectează valabilitatea atestatului sau de un incident de securitate care îl afectează; unitatea de portofel a fost suspendată sau revocată (revocare imediată, secțiunea 11.3) ori cheia titularului a fost compromisă; subiectul a decedat sau a fost radiat (ETSI TS 119 471, REQ-EAASP-4.2.5.1-05);

– revocarea se efectuează în cel mult 24 de ore de la primirea cererii sau de la luarea la cunoștință a motivului, iar la suspendarea sau revocarea unității de portofel, imediat (secțiunea 11.3); când un atestat face parte dintr-un lot, se revocă întregul lot; titularul este informat, iar, când este posibil, sunt informați și solicitantul, dacă este altă persoană decât titularul, și, pentru

atestatele emise în baza contractului-cadru, persoana juridică parte la contract, la datele de contact cunoscute (ETSI TS 119 471, REQ-EAASP-4.2.5.1-06); revocarea este gratuită;

– listele de stare sunt sigilate de CERTDIGITAL (integritate și autenticitate, art. 4 alin. (5)), nu conțin date cu caracter personal, se actualizează cel puțin o dată la 24 de ore și imediat după fiecare revocare și sunt disponibile public, 24/7; durata maximă de indisponibilitate este stabilită în secțiunea 12.6;

– tehnicile de revocare respectă confidențialitatea și împiedică stabilirea de legături și trasabilitatea (art. 4 alin. (4)): CERTDIGITAL nu află când, unde sau față de cine este prezentat un atestat.

6.8. Separarea serviciului și protecția vieții private

– CERTDIGITAL **nu combină** datele cu caracter personal referitoare la serviciu cu date cu caracter personal provenite din alte servicii proprii sau ale partenerilor comerciali (art. 45h alin. (1));

– datele serviciului se păstrează **separate logic** de celelalte date deținute de CERTDIGITAL (art. 45h alin. (2));

– serviciul se prestează **separat din punct de vedere funcțional** de celelalte servicii (art. 45h alin. (3)): componente, baze de date, chei și drepturi de acces dedicate. Când identitatea se verifică printr-un certificat calificat CertDigital, serviciul validează certificatul sau semnătura prezentate de solicitant, fără acces la evidențele autorității de certificare;

– se prelucrează numai datele necesare emiterii, iar înainte de punerea în funcțiune se efectuează evaluarea impactului asupra protecției datelor (art. 35 din Regulamentul (UE) 2016/679).

6.9. Timpul de încredere și jurnalele

– serverele serviciului sunt sincronizate cu o sursă de timp legată de UTC;

– se jurnalizează cererile, verificările identității și ale atributelor (cu sursa și rezultatul), emiterile, revocările, publicarea listelor de stare, operațiile administrative și evenimentele de securitate, conform ETSI EN 319 401 și TS 119 471; jurnalele nu conțin informații despre utilizarea atestatelor;

– evenimentele de securitate jurnalizate cuprind toate încercările de autentificare, reușite și eșuate, la platforma de emitere și la interfețele de administrare, modificările politicii de securitate și ale configurației, pornirea și oprirea sistemelor, căderile sistemelor și defecțiunile hardware, activitatea firewall-urilor și a routerelor și încercările de acces la resursele serviciului (ETSI TS 119 471, REQ-EAASP-7.4-04, 7.10-03);

– aceste evenimente se monitorizează continuu; încercările de acces neautorizat sau neobișnuite și încercările de autentificare eșuate repetate generează alerte transmise fără întârziere

personalului de serviciu, iar evenimentul se înregistrează și se tratează conform Procedurii de notificare a incidentelor (ETSI TS 119 471, REQ-EAASP-7.4-03);

– dovezile verificărilor și evidența atestatelor emise se păstrează cel puțin 10 ani de la expirarea atestatului.

6.10. Personalul

Personalul cu roluri de încredere este angajat al CENTRUL DE CALCUL S.A. și are cunoștințele, experiența și calificările necesare, dovedite prin instruire formală, atestări sau experiență practică, și primește cel puțin o dată la 12 luni instruire privind amenințările noi și practicile de securitate actuale. Rolurile serviciului sunt separate de cele ale altor servicii, în măsura cerută de art. 45h alin. (3).

6.11. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital, cu următoarele precizări:

– serviciul este operat în centrul de date principal și în centrul de date secundar, conform Procedurii DRP (PO_SI_63), cu durata maximă de restabilire de 24 de ore pentru emitere și de 4 ore pentru listele de stare și cu pierderea maximă de date de cel mult 5 minute;

– 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;

– la compromiterea sau la suspiciunea de compromitere a cheii CERTDIGITAL QEAA SERVICE G5, CERTDIGITAL oprește emiterea, revocă toate atestatele emise cu această cheie, iar certificatul de sigiliu al serviciului se revocă de CERTDIGITAL QCA G5; la compromiterea sistemelor serviciului se revocă atestatele afectate. CERTDIGITAL informează, fără întârzieri nejustificate, titularii și, când este posibil, subiecții, beneficiarii contractelor-cadru, părțile care se bazează și celelalte entități cu care are acorduri sau alte relații stabilite, inclusiv ceilalți prestatori de servicii de încredere și furnizorii de portofele, precum și ADR și, după caz, DNSC și ANSPDCP (ETSI TS 119 471, REQ-EAASP-7.11.3-02, 7.11.3-03);

– după un dezastru sau o compromitere, CERTDIGITAL analizează cauzele și aplică măsurile prin care, în măsura posibilului, se evită repetarea lor (ETSI TS 119 471, REQ-EAASP-7.11.3-01);

– monitorizarea securității ține seama de sensibilitatea informațiilor colectate (REQ-EAASP-7.9-02);

– disponibilitatea interfeței de emitere este de cel puțin 99,5%, cu excepția intervențiilor planificate anunțate în prealabil; listele de stare sunt disponibile 24/7.

6.12. Controale criptografice și de rețea

– cheia sigiliului atestatelor se află într-un **dispozitiv calificat de creare a sigiliului**, iar celelalte chei folosite pentru prestarea serviciului se află în dispozitive criptografice certificate Common Criteria EAL4 sau superior, EUCC EAL4 sau superior ori FIPS 140-3 nivel 3 (până la 31.12.2030), configurate conform certificării (REQ-EAASP-7.5.3-02);

– cheile se generează în ceremonie, sub control dual, și se folosesc numai pentru atestate și informațiile de stare;

– tehnicile criptografice respectă documentul „Agreed Cryptographic Mechanisms" al ECCG (REQ-EAASP-7.5.3-01B) și se gestionează pe tot ciclul de viață, cu posibilitatea înlocuirii algoritmilor (REQ-EAASP-7.5.3-01A);

– accesul administrativ folosește autentificare cu mai mulți factori; comunicațiile cu portofelele și cu sursele autentice sunt criptate;

– sistemele serviciului au configurația întărită: conturile, aplicațiile, serviciile, protocoalele și porturile care nu sunt folosite în operarea serviciului se elimină sau se dezactivează, iar configurația se verifică înaintea punerii în funcțiune, la fiecare modificare și cel puțin o dată pe an (ETSI TS 119 471, REQ-EAASP-7.8-03);

– scanarea de vulnerabilități se efectuează 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.

6.13. 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 (REQ-EAASP-6.3-02);

– încetarea se face conform Planului de încetare a serviciilor (00r, anexa A14), elaborat potrivit RE 2025/2530 (REQ-EAASP-7.12-04): emiterea se oprește; informațiile de stare ale atestatelor valabile se mențin disponibile, prin CERTDIGITAL sau prin entitatea desemnată, ori atestatele se revocă, cu informarea titularilor; listele de stare, evidența atestatelor emise și a revocărilor, dovezile verificărilor și jurnalele serviciului se predau entității desemnate, pentru durata de păstrare rămasă (secțiunea 13.3); cererile respinse nu se predau și se șterg la data încetării; celelalte date ale serviciului, păstrate separat (art. 45h), se șterg; cheile serviciului se distrug.

6.14. Evaluarea conformității

Serviciul este evaluat de un organism de evaluare a conformității acreditat conform RE 2025/2162, înainte de începerea prestării și apoi 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

– verifică identitatea și atributele conform art. 24 alin. (1)–(1b) și emite numai atestate cu atribute verificate;

– emite atestate care îndeplinesc anexa V, în formatele din anexa II la RE 2024/2979;

– revocă atestatele în cazurile și termenele din secțiunea 6.7 și publică informațiile de stare 24/7;

– respectă art. 45h și nu urmărește utilizarea atestatelor;

– publică documentația serviciului 24/7.

7.2. Obligațiile solicitantului, ale subiectului și ale titularului

– furnizează informații complete și corecte și dovedesc dreptul de reprezentare, dacă este cazul;

– protejează portofelul și mijloacele de autentificare și cer fără întârziere revocarea dacă atributele nu mai sunt corecte sau dacă portofelul ori cheile au fost compromise;

– prezintă atestatele numai pe durata valabilității lor și numai în scopuri legale, conform termenilor și condițiilor;

– reprezentantul legal care deține un atestat A.2 în numele persoanei juridice îl prezintă numai în numele acesteia (secțiunea 6.3.1).

7.3. Obligațiile părților care se bazează

– verifică sigiliul electronic calificat al atestatului și statutul calificat al serviciului în Lista de încredere a României;

– verifică perioada de valabilitate, starea atestatului în lista de stare și legarea de titular;

– folosesc atributele numai în limita domeniului lor de aplicare și a scopului declarat, cu respectarea art. 45c.

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: erorile din sursele autentice pe care CERTDIGITAL nu le putea detecta prin verificarea prevăzută în politica atestatului; informațiile false furnizate de solicitant; compromiterea portofelului sau a cheilor titularului, nenotificată; utilizarea atestatului după expirare sau revocare ori în afara domeniului său de aplicare; utilizarea serviciului peste limitările notificate în prealabil și recognoscibile de terți; forța majoră.

Nicio prevedere nu exclude și nu limitează răspunderea pentru intenție sau culpă gravă (art. 1355 Cod civil); în raporturile cu consumatorii se aplică Legea nr. 193/2000.

7.5. Asigurarea

CENTRUL DE CALCUL S.A. deține, pentru serviciul de atestare electronică calificată a atributelor, 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 pentru emiterea atestatelor sunt cele din lista publicată pe site-ul https://www.certdigital.ro/ sau din oferta transmisă la cerere (art. 11 alin. (1) din Legea nr. 214/2024). Revocarea și consultarea informațiilor de stare sunt gratuite.

8.2. Protecția datelor cu caracter personal

CERTDIGITAL este **operator** pentru datele prelucrate în cadrul serviciului, conform Politicii de protecție a datelor (00d), cu respectarea art. 45h din Regulamentul eIDAS (secțiunea 6.8). Datele se prelucrează pentru executarea serviciului solicitat și pentru îndeplinirea obligațiilor legale de păstrare (art. 6 alin. (1) lit. (b) și (c) 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). Titularii 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

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 eIDAS și ale regulamentelor de punere în aplicare

9.1. Tabel de corespondență

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 24 alin. (1), (1a), (1b)	verificarea identității și a atributelor	6.4, 6.5
art. 45b alin. (2); art. 45c	efectul juridic; limita privind identificarea electronică	1.4
art. 45d alin. (1)–(3); anexa V lit. (a)–(i)	conținutul atestatului calificat	4.5, 6.6
art. 45d alin. (4)	revocarea definitivă	6.7
art. 45e; RE 2025/1569, art. 9	verificarea în raport cu sursele autentice	6.5
art. 45g	interfața cu portofelele europene pentru identitatea digitală	4.2
art. 45h alin. (1)–(3)	necombinarea datelor; separarea logică și funcțională	6.8, 6.10
RE 2025/1569, art. 3 alin. (1), anexa I (TS 119 471 V1.1.1 adaptat)	cerințele pentru prestator	1.2, 6.1–6.14
RE 2025/1569, art. 3 alin. (2)	sistemele de atestare din catalog	4.4, 5.1
RE 2025/1569, art. 4 alin. (2)–(5); anexa II	revocarea; tehnici care împiedică trasabilitatea; integritatea informațiilor de stare	6.7
RE 2024/2979, anexa II (TS 119 472-1 V1.2.1, cl. 2–6, adaptat prin RE 2026/1731)	formatele SD-JWT VC și mdoc; stare fără suspendare; nu se emit atestate de scurtă durată	4.3, 6.6, 6.7
RE 2024/2982 (TS 119 472-3 V1.1.1); RE 2025/848	emiterea în portofel; înregistrarea ca parte care se bazează pe portofel	4.2
RE 2025/1566 (TS 119 461 V2.1.1)	verificarea identității, din 19.08.2027	6.4
TS 119 471: REQ-EAASP-4.2.2.3-02, -03	certificat de acces; validarea unității de portofel	4.2
TS 119 471: REQ-EAASP-4.2.2.1-09	emiterea conform politicii serviciului și politicii atestatului	6.6, anexa A
TS 119 471: REQ-EAASP-4.2.2.3-06	legarea de portofel, obligatorie pentru toate tipurile de atestat	6.6, anexa A
TS 119 471: REQ-EAASP-4.2.3.1-02	controlul exclusiv al subiectului și excepțiile stabilite de politică	6.3.1
TS 119 471: REQ-EAASP-4.2.5.1-04; REQ-EAASP-4.2.5.2-06	nu se emit atestate de scurtă durată; toate atestatele pot fi revocate și conțin informații de stare	6.7, 12.6
TS 119 471: REQ-EAASP-6.1-02	mecanismul de revocare descris în declarația de practici (Partea a II-a)	6.7, 12.6
TS 119 471: REQ-EAASP-6.3-02; REQ-EAASP-7.12-04	notificări ADR (o lună / trei luni); planul de încetare	6.13
TS 119 471: REQ-EAASP-7.5.3-01A, -01B, -02	agilitate criptografică; ECCG ACM; sigiliul pe dispozitiv calificat	4.5, 6.12
TS 119 471: REQ-EAASP-7.9-02	monitorizarea ține seama de sensibilitatea datelor	6.11
ETSI TS 119 412-6, cl. 7	profilul certificatului de sigiliu	4.5
RE 2025/2530	notificări ADR; plan de încetare	6.13

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

PARTEA A II-A – Declarația de practici

10. Publicare și depozit

Partea a II-a este declarația de practici a serviciului (ETSI TS 119 471 V1.1.1, cu adaptările din anexa I la RE 2025/1569, astfel cum a fost modificat prin RE 2026/1735). Ea descrie modul în care CERTDIGITAL pune în aplicare politica din Partea I și politicile atestatelor din anexa A, cu schema atributelor din anexa C. Identificarea documentului, participanții și furnizorii externi, utilizarea serviciului și referințele normative sunt cele din Partea I (secțiunile 1.2–1.4 și capitolul 2); corespondența practicilor cu cerințele este în anexa B.

La https://www.certdigital.ro/repository/ se publică, 24/7: prezentul document, cu politicile atestatelor (anexa A), termenii și condițiile, descrierea fiecărui tip de atestat (identificatorul tipului, atributele, sistemul de atestare și metadatele tipului), certificatele serviciului și lanțul lor, adresele listelor de stare și durata maximă de indisponibilitate a acestora. Metadatele emitentului, cerute de protocolul de emitere, se publică la punctul de acces al serviciului. Versiunile anterioare ale documentelor rămân disponibile în secțiunea „Arhivă”.

11. Interfața cu portofelele

11.1. Fluxul de emitere

Emiterea folosește protocolul OpenID for Verifiable Credential Issuance, în profilul din ETSI TS 119 472-3 V1.1.1:

1. utilizatorul alege tipul de atestat, pornind din portofel sau de pe site-ul CERTDIGITAL, și acceptă termenii și condițiile;

2. portofelul trimite cererea de autorizare împreună cu atestatul unității de portofel; CERTDIGITAL validează unitatea de portofel (secțiunea 11.3);

3. CERTDIGITAL verifică identitatea utilizatorului (secțiunea 12.2) și, la cererea acestuia, atributele la sursă (secțiunea 12.3);

4. portofelul trimite cererea de emitere, cu dovada posesiei cheilor pe care se leagă atestatul și cu atestatul cheilor;

5. CERTDIGITAL emite atestatul sau lotul de atestate (secțiunea 12.4). Dacă verificarea la sursă nu se poate încheia imediat, emiterea este amânată, iar portofelul primește atestatul ulterior, pe baza identificatorului tranzacției.

11.2. Autentificarea reciprocă și înregistrarea

CERTDIGITAL este înregistrată ca parte care se bazează pe portofel, cu dreptul de furnizor de atestate calificate (RE 2025/848, modificat prin RE 2026/1730), și se autentifică față de unitatea de portofel cu un certificat de acces valabil (REQ-EAASP-4.2.2.3-02). Metadatele emitentului sunt semnate cu cheia certificatului de acces, care se include în metadate (antetul `x5c`), conform ETSI TS 119 472-3 V1.1.1 (REQ-EAASP-4.2.2.3-08); ele conțin și certificatul de înregistrare, dacă acesta este emis. Cheile asociate certificatelor de acces se păstrează în dispozitive criptografice certificate (secțiunea 14).

11.3. Validarea unității de portofel

La fiecare emitere, CERTDIGITAL verifică (REQ-EAASP-4.2.2.3-03):

– semnătura atestatului unității de portofel și a atestatului cheilor, cu încrederea ancorată în lista de încredere a furnizorilor de portofele publicată de Comisie;

– dovada posesiei cheii private corespunzătoare cheii publice din atestatul unității de portofel și dovada posesiei cheilor atestate, pe care se leagă atestatul, prezentate de dispozitivul securizat al portofelului (REQ-EAASP-4.2.2.3-04);

– faptul că unitatea de portofel și cheile ei nu au fost suspendate sau revocate și că cheile se află în dispozitivul criptografic securizat al portofelului (WSCD), la nivelul cerut de politica atestatului (anexa A, rândul „Legarea de portofel”: nivelul corespunzător nivelului de

asigurare ridicat), dovedit prin atestatul cheilor; dacă nivelul nu este dovedit, atestatul nu se emite (REQ-EAASP-4.2.1.2-03).

Pe durata valabilității atestatelor, CERTDIGITAL verifică cel puțin o dată la 24 de ore starea unității de portofel și a cheilor pe care sunt legate atestatele; dacă furnizorul portofelului a suspendat sau a revocat unitatea de portofel ori cheile ei, CERTDIGITAL revocă imediat, automat, la constatarea stării, toate atestatele emise în acea unitate de portofel, fără a aștepta termenul de la secțiunea 12.6 (ETSI TS 119 471, REQ-EAASP-4.2.5.2-04).

11.4. Limite

Un lot cuprinde cel mult 10 atestate; numărul de cereri pe unitatea de timp se stabilește prin contract, iar disponibilitatea interfeței este publicată în termenii și condițiile serviciului.

12. Ciclul de viață al atestatului

12.1. Cererea

Atestatul se emite numai la cererea utilizatorului, după acceptarea termenilor și condițiilor, care se înregistrează. Cererea stabilește tipul de atestat și subiectul; când subiectul este o persoană juridică, solicitantul trebuie să fie reprezentantul ei legal, verificat conform anexei A.1.

12.2. Verificarea identității

Metoda (art. 24 alin. (1a))	Aplicarea la CERTDIGITAL
(a) portofelul european pentru identitatea digitală sau un mijloc de identificare electronică notificat, cu nivel de asigurare ridicat	prezentarea datelor de identificare personală (PID) din portofel; metoda principală
(b) certificat calificat, semnătură sau sigiliu electronic calificat	semnarea cererii cu o semnătură electronică calificată; certificatul și semnătura se validează de componenta de validare a serviciului, fără acces la evidențele autorității de certificare (art. 45h)
(c) alte metode de încredere ridicată, confirmate de un organism de evaluare a conformității	identificarea la distanță CERTDIGITAL KYC
(d) prezența fizică	la sediul CERTDIGITAL, cu actul de identitate

La metodele (c) și (d) se aplică procedurile de verificare a identității folosite de CERTDIGITAL și pentru certificatele calificate: la prezența fizică, la sediul CERTDIGITAL, operatorul de verificare a identității CERTDIGITAL verifică actul de identitate conform pasului 2 din Regulamentul privind identificarea și cererea certificatelor digitale calificate (RIS), versiunea 1.4 din 03.11.2026, iar documentele de identitate acceptate sunt cele din anexa 1 a acestuia; verificarea se face numai de personalul CERTDIGITAL, fără parteneri mandatați, deoarece CERTDIGITAL nu deleagă terților verificarea identității pentru acest serviciu (secțiunea 14.5); la CERTDIGITAL KYC, verificarea înregistrării video de către operatorul de validare CERTDIGITAL se face conform Procedurii de lucru privind identificarea video la distanță – Operatori (PIV), referința 18/2026, versiunea 1.1 din 14.07.2026, iar fluxul complet al soluției CERTDIGITAL KYC este descris în Descrierea procesului de identificare video la distanță (DIV), referința 11/2026, versiunea 1.2 din 14.07.2026. Trimiterile la regulamentele interne indică versiunea în vigoare la data aprobării prezentului document. O versiune nouă a unui regulament se aplică după instruirea operatorilor și se preia în prezentul document la versiunea lui următoare. De la 19.08.2027, verificarea identității, prin oricare dintre metodele de mai sus, respectă ETSI TS 119 461 V2.1.1, cu adaptările din RE 2025/1566 (secțiunea 6.4). Metoda, dovezile și momentul verificării se înregistrează.

Înainte de emiterea atestatului în portofel, CERTDIGITAL primește de la unitatea de portofel datele de identificare personală ale titularului (PID) sau, pentru portofelul unei persoane juridice, datele de identificare ale persoanei juridice (LPID) și le verifică și validează: sigiliul furnizorului de PID, cu încrederea ancorată în lista de încredere a furnizorilor de PID publicată de Comisie; perioada de valabilitate; starea (nerevocat); legarea de unitatea de portofel care le prezintă, prin dovada

posesiei cheii. Când identitatea solicitantului se verifică prin una dintre metodele (b)–(d), datele PID primite de la unitatea de portofel se compară cu identitatea verificată. Dacă oricare dintre verificări eșuează, atestatul nu se emite (ETSI TS 119 471, REQ-EAASP-4.2.2.3-01).

12.3. Verificarea atributelor

– atributele se verifică numai la cererea utilizatorului și numai pentru tipul de atestat solicitat;

– pentru atestatele din anexa A, CERTDIGITAL obține electronic de la ONRC informațiile din registrul comerțului privind persoana juridică și reprezentanții ei, verifică autenticitatea și originea lor (semnătura sau sigiliul electronic ori canalul autentificat al ONRC) și compară datele de identificare ale subiectului cu cele din registru. Codul numeric personal se folosește numai pentru această comparație și nu se înscrie în atestat. Datele ONRC se obțin prin serviciile online ale ONRC, cu un cont de utilizator autentificat (secțiunea 6.5);

– după ce România pune la dispoziție mecanismul național de verificare (art. 45e; art. 9 din RE 2025/1569; interfața conform ETSI TS 119 478 V1.1.1, din 01.01.2027), atributele se verifică prin acesta; rezultatul este semnat sau sigilat de sursă și se păstrează;

– pentru fiecare atribut se înregistrează: sursa, metoda, momentul, rezultatul și amprenta dovezii;

– pe durata valabilității atestatelor, atributele se reverifică la sursă zilnic, iar pentru atestatele A.2 deținute de un reprezentant legal se reverifică și calitatea acestuia; orice neconcordanță duce la revocare (secțiunea 12.6).

12.4. Emiterea și conținutul atestatului

Element (anexa V)	SD-JWT VC (TS 119 472-1, cl. 5)	mdoc (TS 119 472-1, cl. 6)
(a) mențiunea de atestat calificat	categoria `urn:etsi:esi:eaa:eu:qualified`	aceeași categorie
(b) prestatorul	emitentul (`iss`) și datele emitentului: RO, CENTRUL DE CALCUL S.A., VATRO-2163993	datele emitentului din certificatul inclus în semnătura COSE
(c) subiectul	datele de identificare ale subiectului, conform politicii atestatului	elemente de date în spațiul de nume al tipului
(d) atributele și domeniul lor	revendicări divulgabile selectiv	elemente de date divulgabile selectiv
(e) valabilitatea	momentul emiterii și expirarea, în UTC	`validFrom` și `validUntil`
(f) identificatorul și sistemul	identificator unic; tipul (`vct`), legat de sistemul de atestare	identificator unic; tipul documentului (`docType`)
(g) sigiliul calificat	semnătură JWS (JAdES), cu cheia CERTDIGITAL QEAA SERVICE G5	semnătură COSE asupra obiectului de securitate (MSO), cu aceeași cheie
(h) certificatul	`x5u` și `x5t#S256`, plus lanțul de certificate (`x5c`)	adresa certificatului, amprenta SHA-256 și lanțul de certificate
(i) informațiile de stare	punctele OCSP și CRL din certificatul de sigiliu; în toate atestatele, referința `status` (adresa listei și poziția)	referința de stare din MSO (listă de stare sau listă de identificatori)

Element (anexa V)	SD-JWT VC (TS 119 472-1, cl. 5)	mdoc (TS 119 472-1, cl. 6)
Legarea de titular	`cnf` – cheia unității de portofel	`deviceKeyInfo` – cheia unității de portofel

Valabilitatea începe cel mai devreme la momentul emiterii și nu depășește valabilitatea maximă din politica atestatului. CERTDIGITAL nu folosește pseudonime și nu include în atestat alte date decât cele prevăzute în politica lui. Numele revendicărilor, identificatorii elementelor mdoc, tipurile de date și codificarea atributelor sunt cele din anexa C.

12.5. Legarea de titular, loturile, reemiterea și reînnoirea

– fiecare atestat se leagă de o cheie distinctă a unității de portofel, a cărei posesie se dovedește la emitere;

– la cerere, CERTDIGITAL emite un lot de atestate identice ca atribute, cu chei, identificatori și poziții în lista de stare distincte, destinate unei singure utilizări fiecare, pentru a împiedica corelarea prezentărilor;

– reemiterea: un lot nou pentru aceleași atribute se poate emite în perioada de valabilitate inițială, după autentificarea titularului, fără prelungirea valabilității; reemiterea nu este reînnoire;

– reînnoirea: cererea de reînnoire a unui atestat se face de titular, din portofel, prin fluxul de la secțiunea 11.1, după autentificarea lui. Înainte de reînnoire, CERTDIGITAL verifică faptul că atestatul care se reînnoiește este valabil, adică nu a expirat și nu a fost revocat, și că informațiile folosite la verificarea identității și a atributelor subiectului sunt încă valabile: mijlocul folosit la verificarea identității (datele de identificare personală din portofel sau certificatul calificat) nu a expirat și nu a fost revocat, altfel identitatea se verifică din nou conform secțiunii 12.2, iar atributele se reverifică la sursa autentică, conform politicii atestatului (anexa A). Reînnoirea este o emitere nouă, cu valabilitate, identificator și poziție în lista de stare noi; cererea de reînnoire se jurnalizează (secțiunea 13.3). Pentru un atestat expirat sau revocat nu se face reînnoire, ci o cerere nouă, conform secțiunii 12.1 (ETSI TS 119 471, REQ-EAAS-4.2.4.1-01, REQ-EAASP-4.2.4.1-02).

12.6. Revocarea și informațiile de stare

– **mecanismul** (REQ-EAASP-6.1-02): liste de stare conform IETF Token Status List (draft-ietf-oauth-status-list-20), cu un bit pe poziție și numai două valori, nerevocat (0) și revocat (1). Pentru SD-JWT VC, lista se publică într-un token JWT, iar pentru mdoc într-un token CWT sau ca listă de identificatori. Tokenurile sunt sigilate de CERTDIGITAL și au o valabilitate de cel mult 24 de ore;

– **confidențialitatea**: listele au cel puțin 100.000 de poziții, alocate aleatoriu, nu conțin date cu caracter personal și se publică la adrese statice, fără jurnalizarea pozițiilor consultate;

– **cererile de revocare** se pot face din portofel, din contul de pe site-ul CERTDIGITAL (cu autentificare prin portofel sau prin semnătură electronică calificată), prin e-mail semnat cu semnătură electronică calificată sau la sediul CERTDIGITAL; canalele electronice sunt disponibile 24/7, iar identitatea solicitantului se verifică;

– **termenul**: revocarea se efectuează în cel mult 24 de ore de la primirea cererii sau de la luarea la cunoștință a motivului, inclusiv a rezultatului reverificării la sursă; la suspendarea sau revocarea unității de portofel, revocarea este imediată (secțiunea 11.3); întregul lot se revocă;

– **informarea**: titularul este informat, iar, când este posibil, sunt informați și solicitantul, dacă este altă persoană decât titularul, și, pentru atestatele emise în baza contractului-cadru, persoana juridică parte la contract, la datele de contact cunoscute (ETSI TS 119 471, REQ-EAASP-4.2.5.1-06);

– **actualizarea**: listele se republică cel puțin o dată la 24 de ore și imediat după fiecare revocare;

– **disponibilitatea**: listele de stare sunt servite din ambele centre de date; durata maximă de indisponibilitate este de 4 ore pe incident;

– **atestatele de scurtă durată**: CERTDIGITAL nu emite atestate de scurtă durată; toate atestatele conțin informații de stare și pot fi revocate atât la cerere, cât și din inițiativa CERTDIGITAL. Prin urmare, nu există niciun tip de atestat care să nu poată fi revocat prin serviciul de revocare și niciunul care să nu poată fi revocat din inițiativa CERTDIGITAL (ETSI TS 119 471, REQ-EAASP-4.2.5.1-04), iar informațiile de revocare (adresa listei de stare și poziția atestatului în listă) nu se omit din niciun atestat, indiferent de perioada lui de valabilitate (REQ-EAASP-4.2.5.2-05, -06).

13. Datele, separarea și păstrarea

13.1. Separarea serviciului (art. 45h)

– aplicația, baza de date, cheile de criptare a datelor și conturile tehnice ale serviciului sunt dedicate, iar serviciul rulează într-un segment de rețea separat;

– serviciul nu are interfețe cu bazele de date ale autorității de certificare, ale serviciului de identificare la distanță sau ale altor servicii. Datele primite de la acestea se folosesc numai dacă sunt prezentate de solicitant, ca orice altă dovadă;

– datele serviciului nu se folosesc în alte scopuri și nu se transmit partenerilor comerciali;

– accesul personalului la datele serviciului se acordă numai rolurilor serviciului.

13.2. Riscul de corelare

Riscul ca atestatele să permită urmărirea titularului de către CERTDIGITAL, ca prestator, sau prin colaborarea CERTDIGITAL cu părțile care se bazează (Attestation Provider linkability) se tratează prin următoarele măsuri: loturi de atestate de unică folosință; poziții aleatorii în liste de stare mari; liste servite fără jurnalizarea pozițiilor; CERTDIGITAL nu este contactată la prezentarea atestatului; atestatele conțin numai atributele necesare, divulgabile selectiv.

CERTDIGITAL nu colaborează cu părțile care se bazează pentru urmărirea titularilor: nu primește de la acestea informații despre prezentarea atestatelor, nu le furnizează date din evidența atestatelor emise, în afara informațiilor de stare publice, și nu încheie acorduri care să permită corelarea emiterii cu prezentarea. Datele serviciului nu se folosesc în alte scopuri și nu se transmit partenerilor comerciali (secțiunea 13.1). Personalul cu roluri în serviciu are interdicția, prin fișa postului și prin angajamentul de confidențialitate, de a furniza astfel de informații; încălcarea interdicției se tratează ca incident de securitate. Riscul este evaluat în documentul de gestionare a riscurilor serviciilor de încredere (GR-TSP), ca risc distinct, „corelarea prezentărilor atestatelor de către prestator sau în colaborare cu părțile care se bazează”, și se reevaluează cel puțin o dată pe an (ETSI TS 119 471, REQ-EAASP-6.1.2-01).

13.3. Durata păstrării

Ce se păstrează	Cât	Se predă prin planul de încetare (00r, anexa A14)
dovezile verificării identității și a atributelor (procesul de emitere)	cel puțin 10 ani de la expirarea atestatului	da, entității desemnate, pentru durata de păstrare rămasă
evidența atestatelor emise (tipul, atributele, valabilitatea, poziția în lista de stare, cheia de legare) și a revocărilor, cu înregistrarea acceptării termenilor și condițiilor	cel puțin 10 ani de la expirarea atestatului	da, entității desemnate, pentru durata de păstrare rămasă

Ce se păstrează	Cât	Se predă prin planul de încetare (00r, anexa A14)
jurnalele serviciului: evenimentele de securitate, cererile de emitere și de reînnoire, verificările, evenimentele din ciclul de viață al atestatelor, cererile de revocare și acțiunile rezultate, publicarea listelor de stare, operațiile administrative	cel puțin 10 ani	da, entității desemnate, pentru durata de păstrare rămasă
listele de stare	până la expirarea ultimului atestat pe care îl cuprind	da; entitatea desemnată le menține disponibile până la expirarea ultimului atestat valabil
cererile respinse, cu motivul respingerii și cu înregistrarea acceptării termenilor și condițiilor	1 an de la respingere	nu; se șterg la expirarea termenului de 1 an sau, la încetare, la data încetării

Tabelul acoperă informațiile prevăzute la ETSI TS 119 471, REQ-EAASP-7.10-02 – 7.10-07; duratele și informațiile care se predau la încetare sunt stabilite conform REQ-EAASP-7.10-08. Informațiile înregistrate sunt accesibile numai rolurilor de încredere ale serviciului, în limita atribuțiilor lor, și, la cerere, organismului de evaluare a conformității, ADR și autorităților îndreptățite potrivit legii; persoana vizată are acces la datele care o privesc, conform secțiunii 13.4 (REQ-EAASP-7.10-05).

13.4. Protecția datelor

CERTDIGITAL este operator pentru datele serviciului (Politica de protecție a datelor, 00d). Înainte de punerea în funcțiune se efectuează evaluarea impactului asupra protecției datelor (art. 35 din Regulamentul (UE) 2016/679). Datele nu se transferă în afara Uniunii Europene.

14. Controale de management și operare

Se aplică Politicile generale CertDigital și ETSI EN 319 401 V3.2.1, cu adaptările din RE 2026/1735:

– **cheia sigiliului**: certificatul CERTDIGITAL QEAA SERVICE G5, cu cheie ECDSA P-256, cerută de formatul mdoc și de algoritmul ES256. Cheia se generează în ceremonie, sub control dual, în modulul Thales Luna PCIe HSM 7 A790, certificat ca dispozitiv calificat de creare a sigiliului (eIDAS-2400055-01), Common Criteria (NSCIB-CC-2400054-01) și FIPS 140-3 nivel 3. Cheia se folosește numai pentru atestate și listele de stare (REQ-EAASP-7.5.3-02);

– **celelalte chei** (certificatele de acces, TLS) se păstrează în dispozitive criptografice certificate CC/EUCC EAL4+ sau FIPS 140-3 nivel 3; cheile certificatelor de acces se generează, se folosesc, se copiază și se distrug conform Procedurii privind generarea cheilor, document intern (ETSI TS 119 471, REQ-EAASP-7.5.5-06);

– **criptografia**: conform ECCG „Agreed Cryptographic Mechanisms”, cu revizuire anuală și plan de înlocuire a algoritmilor (REQ-EAASP-7.5.3-01A, -01B);

– **gestionarea schimbărilor**: modificările platformei, ale tipurilor de atestat și ale configurației se testează și se aprobă înainte de producție; vulnerabilitățile se remediază prompt;

– **personalul**: roluri de încredere separate, rezervate serviciului; instruire cel puțin o dată la 12 luni;

– **rețeaua**: autentificare cu mai mulți factori pentru accesul administrativ, canale criptate, scanare de vulnerabilități cel puțin trimestrială, test de penetrare cel puțin anual, firewall-uri restrictive, configurația întărită a sistemelor (secțiunea 6.12);

– **jurnalizarea**: cererile, verificările, emiterile, revocările, publicarea listelor de stare, operațiile administrative și evenimentele de securitate, inclusiv încercările de autentificare reușite și eșuate, cu monitorizare continuă și alertare (secțiunea 6.9); monitorizarea ține seama de sensibilitatea datelor (REQ-EAASP-7.9-02);

– **continuitatea**: centrul de date principal și centrul de date secundar, conform PO_SI_63;

– **lanțul de aprovizionare**: furnizorul platformei de emitere și componentele software sunt evaluate înainte de utilizare;

– **incidentele**: notificate conform 00q; la compromiterea cheii de sigiliu sau a sistemelor serviciului se aplică secțiunea 6.11;

– **încetarea**: conform planului 00r, anexa A14 (RE 2025/2530): informațiile marcate „da” în tabelul de la secțiunea 13.3 se predau entității desemnate, cererile respinse se șterg la data încetării, iar cheile se distrug;

– **conformitatea**: evaluare de către un CAB acreditat înainte de începerea prestării și apoi cel puțin o dată la 24 de luni, inclusiv pentru procedurile privind sistemele de atestare (art. 3 alin. (2) din RE 2025/1569); audit intern anual.

14.1. Securitatea rețelei

Pe lângă măsurile din Politicile generale (cap. 9), din planul de securitate al sistemului informatic și din secțiunea 6.12, pentru serviciu se aplică următoarele (ETSI EN 319 401, cl. 7.8):

– Toate sistemele dintr-o zonă de securitate au aceleași controale de securitate: configurația întărită, protecția anti-malware, jurnalizarea centralizată și regulile de filtrare ale zonei; un sistem care cere alte controale se mută într-o zonă proprie. Accesul la o rețea sau la o zonă se acordă pe baza evaluării cerințelor ei de securitate (GR-TSP), cu aprobarea ofițerului de securitate IT (REQ-7.8-03).

– Comunicațiile dintre zone și, în interiorul fiecărei zone, dintre sisteme se limitează la cele necesare funcționării serviciului, prin firewall-uri cu filtrare și monitorizare și prin reguli de filtrare la nivelul platformei de virtualizare și al containerelor; restul traficului este blocat (REQ-7.8-04).

– Conexiunile și serviciile care nu sunt necesare se interzic sau se dezactivează pe toate sistemele (porturi, protocoale, servicii și conturi implicite); la rețeaua CERTDIGITAL și la sistemele serviciului se conectează numai echipamente autorizate și înscrise în inventar (REQ-7.8-05).

– Regulile firewall, segmentarea rețelei și măsurile de protecție se revizuiesc cel puțin anual, după incidente semnificative și după modificări semnificative ale operațiunilor sau ale riscurilor; revizuirea se consemnează în proces-verbal (REQ-7.8-06).

– Rețeaua de administrare este separată de rețeaua operațională, iar canalele de administrare sunt separate de restul traficului. Stațiile de administrare sunt dedicate: se folosesc numai pentru administrarea sistemelor și a măsurilor de securitate, nu pentru e-mail, navigare pe internet sau alte activități (REQ-7.8-08, REQ-7.8-09).

– Comunicațiile dintre sisteme de încredere distincte (aplicațiile și modulele criptografice, aplicațiile și bazele de date, cele două centre de date) se fac numai prin canale separate logic de celelalte comunicații, criptate și cu autentificarea reciprocă a capetelor, prin TLS sau VPN cu certificate (REQ-7.8-11).

– Mediile de dezvoltare, de test și de producție sunt separate, inclusiv copiile lor de siguranță: copiile mediilor de dezvoltare și de test se păstrează separat de copiile sistemelor de producție, în depozite la care sistemele de producție nu au acces (REQ-7.8-10).

– Protecția împotriva programelor malițioase este activă pe toate stațiile și serverele; semnăturile și motorul de detecție se actualizează automat, cel puțin o dată pe zi, iar consola centrală semnalează sistemele neactualizate în ultimele 24 de ore (REQ-7.8-16, REQ-7.8-17).

– Scanările de vulnerabilitate acoperă adresele IP publice și private ale sistemelor serviciului, din lista ținută de ofițerul de securitate IT și actualizată la fiecare modificare a infrastructurii. Pentru fiecare scanare de vulnerabilități și pentru fiecare test de penetrare se păstrează, împreună cu raportul, dovezile că a fost efectuat de o persoană sau entitate cu competențele, instrumentele, experiența, angajamentul deontologic și independența necesare unui raport credibil: calificările și certificările profesionale ale echipei, instrumentele folosite și declarația de independență față de activitatea testată (REQ-7.8-13, REQ-7.8-20).

– CERTDIGITAL aplică un plan de implementare, aprobat de Directorul General, pentru: a) trecerea treptată și sigură la protocoalele de rețea de ultimă generație (IPv6, în regim dual-stack, pentru punctele de acces publice), cu măsuri de accelerare a trecerii; b) standardele moderne de securitate a e-mailului pentru toate domeniile de e-mail ale CERTDIGITAL (SPF, DKIM și DMARC cu politică de respingere, MTA-STS și TLS-RPT; DANE, unde infrastructura permite); c) bunele practici de securitate DNS (DNSSEC pentru zonele certdigital.ro), de securitate a rutării (RPKI, cu înregistrări ROA pentru prefixele folosite, prin furnizorii de internet) și de igienă a rutării, prin filtrarea adreselor sursă false conform BCP 38 (REQ-7.8-23).

14.2. Monitorizarea și jurnalizarea

Monitorizarea și jurnalizarea se fac conform Politicilor generale (secțiunea 9.4), planului de securitate al sistemului informatic și secțiunii 6.9, cu următoarele precizări (ETSI EN 319 401, cl. 7.9.1):

– Jurnalele cuprind cel puțin: a) traficul de rețea de intrare și de ieșire (jurnalele firewall-urilor și ale sistemelor de detecție și prevenire a intruziunilor); b) crearea, modificarea și ștergerea conturilor și extinderea drepturilor; c) accesul la sisteme și aplicații; d) evenimentele de autentificare, reușite și eșuate; e) pornirea, oprirea și suspendarea jurnalizării; f) administrarea utilizatorilor și a drepturilor, inclusiv accesul privilegiat; g) activitățile efectuate cu conturile de administrator; h) accesul la fișierele de configurație critice și la copiile de siguranță și modificarea lor; i) jurnalele instrumentelor de securitate (anti-malware, detecția și prevenirea intruziunilor, firewall-uri); j) utilizarea și performanța resurselor sistemelor; k) accesul fizic în zonele de securitate; l) accesul la echipamentele de rețea și utilizarea lor; m) evenimentele de mediu: alarmele de incendiu, inundație, temperatură, umiditate, alimentare și climatizare (REQ-7.9.1-04).

– Regulile de corelare și pragurile de alertare se ajustează la revizuirea lunară a jurnalelor și după fiecare incident sau alertă falsă, pentru a reduce alertele fals pozitive și evenimentele nedetectate; ajustările se consemnează (REQ-7.9.1-08).

– Lista activelor jurnalizate (sistemele, aplicațiile, echipamentele de rețea și de securitate și categoriile de evenimente colectate de la fiecare) se stabilește pe baza evaluării riscurilor (GR-TSP), face parte din inventarul activelor și se revizuiește, împreună cu procedurile de jurnalizare și monitorizare, cel puțin anual și după incidente semnificative (REQ-7.9.1-09, REQ-7.9.1-16, REQ-7.9.1-18).

– Pragurile de alarmă se stabilesc pentru fiecare categorie monitorizată (disponibilitatea serviciilor și a punctelor de acces, utilizarea resurselor, autentificările eșuate repetate, modificările de configurație și de drepturi, evenimentele de securitate, sincronizarea timpului, parametrii de mediu) și se documentează în configurația sistemului de monitorizare; depășirea unui prag declanșează automat alarma către personalul de serviciu și ofițerul de securitate IT, care inițiază fără întârziere răspunsul, conform Procedurii de notificare a incidentelor (PRO-7.9.1-11 – PRO-7.9.1-13).

– Sistemele de jurnalizare și de monitorizare sunt redundante: rulează pe platforma de virtualizare din ambele centre de date, iar jurnalele se replică în DC2 și se includ în copiile de siguranță. Funcționarea lor este supravegheată de un sistem independent de ele, care alertează personalul de serviciu la oprirea colectării jurnalelor sau a monitorizării (REQ-7.9.1-14, REQ-7.9.1-16, REQ-7.9.1-17).

14.3. Incidentele și vulnerabilitățile

Incidentele se gestionează și se notifică conform Politicilor generale (cap. 10), Procedurii de notificare a incidentelor (00q) și secțiunii 6.11, cu următoarele precizări (ETSI EN 319 401, cl. 7.9.2–7.9.5 și 7.11.3):

– Un incident este semnificativ dacă este îndeplinit cel puțin unul dintre criteriile de mai jos (Regulamentul de punere în aplicare (UE) 2024/2690, art. 3 și 14): a) a cauzat sau poate cauza CERTDIGITAL o pierdere financiară directă mai mare de 500.000 EUR sau de 5 % din cifra de afaceri anuală totală din exercițiul financiar anterior, oricare dintre acestea este mai mică; b) a cauzat sau poate cauza exfiltrarea secretelor comerciale ale CERTDIGITAL; c) a cauzat sau poate cauza decesul unei persoane fizice; d) a cauzat sau poate cauza prejudicii considerabile sănătății unei persoane fizice; e) s-a produs un acces reușit, suspectat a fi rău intenționat și neautorizat, la rețelele și sistemele informatice, care poate cauza perturbări operaționale grave; f) îndeplinește criteriile incidentelor recurente de mai jos; g) un serviciu de încredere este complet indisponibil mai mult de 20 de minute; h) un serviciu de încredere este indisponibil pentru utilizatori sau pentru părțile care se bazează mai mult de o oră, calculat pe o săptămână calendaristică; i) mai mult de 1 % dintre utilizatorii sau părțile care

se bazează din Uniune, ori mai mult de 200.000 dintre aceștia, oricare dintre numere este mai mic, sunt afectați de disponibilitatea limitată a unui serviciu de încredere; j) este compromis accesul fizic într-o zonă în care se află rețelele și sistemele informatice și la care accesul este restricționat personalului de încredere, ori protecția acestui acces; k) este compromisă integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate în legătură cu prestarea unui serviciu de încredere, cu impact asupra a mai mult de 0,1 % dintre utilizatorii sau părțile care se bazează din Uniune ori a mai mult de 100 dintre aceștia, oricare dintre numere este mai mic. Întreruperile programate și consecințele planificate ale lucrărilor de mentenanță programate, efectuate de CERTDIGITAL sau în numele său, nu se consideră incidente semnificative. La calculul numărului de utilizatori afectați se iau în considerare clienții care au un contract cu CERTDIGITAL prin care au acces la rețelele și sistemele informatice sau la serviciile oferite prin acestea, precum și persoanele fizice și juridice asociate clienților persoane juridice care folosesc aceste rețele, sisteme sau servicii. Incidentele care, separat, nu sunt semnificative se consideră împreună un incident semnificativ dacă s-au produs de cel puțin două ori în 6 luni, au aceeași cauză aparentă și, împreună, depășesc pragul pierderii financiare directe de mai sus (REQ-7.9.3-07 – REQ-7.9.3-10).

– Evaluarea și clasificarea evenimentelor se fac după criteriile de mai sus, stabilite în prealabil, și printr-o triere care stabilește prioritatea izolării incidentului și a eliminării cauzei; pentru evaluare se analizează jurnalele relevante, corelate în sistemul centralizat de jurnale. Clasificarea se reevaluează ori de câte ori apar informații noi sau după analiza informațiilor existente; modificarea se consemnează în registrul incidentelor și, dacă este cazul, se comunică destinatarilor notificării. Ofițerul de securitate IT analizează trimestrial registrul incidentelor pentru a identifica incidentele recurente (REQ-7.9.4-02, REQ-7.9.4-04).
– Răspunsul la incident cuprinde izolarea, pentru a împiedica extinderea efectelor, eliminarea cauzei (eradicarea), astfel încât incidentul să nu continue și să nu se repete, și recuperarea, inclusiv prin planul de continuitate; după închidere, analiza post-incident consemnează în registrul incidentelor cauza, lecțiile învățate și măsurile (REQ-7.9.2-16, PRO-7.9.5-06).
– Angajații raportează imediat ofițerului de securitate IT orice eveniment suspect. Clienții, titularii, părțile care se bazează și furnizorii raportează orice eveniment suspect sau posibil incident de securitate la office@certdigital.ro sau la +40 253 214 767, iar suspiciunea de compromitere a mijloacelor de autentificare, a cheilor sau a portofelului se poate transmite oricând și prin canalele de revocare ale serviciului. Canalul se comunică clienților prin prezentul document, prin termenii și condițiile serviciului și prin Politica privind relațiile cu clienții, iar furnizorilor, prin contract; raportările se înregistrează și se transmit imediat ofițerului de securitate IT, iar personalul este instruit, la angajare și cel puțin anual, să folosească procedura și să se adreseze punctului de contact (REQ-7.9.3-03 – PRO-7.9.3-06).

– Ofițerul de securitate IT verifică trimestrial, pe baza registrului incidentelor, că fiecare incident închis are analiza post-incident documentată (cauza, lecțiile învățate, măsurile) și raportează rezultatul Directorului General; verificarea se reia la auditul intern anual. Procedura de gestionare a incidentelor se testează și se revizuiește cel puțin anual, după incidente semnificative și la modificări semnificative ale operațiunilor sau ale riscurilor (REQ-7.9.2-14, REQ-7.9.5-08).

– Avertizările și informările primite de la DNSC, în calitate de CSIRT național, și de la ADR privind incidente, vulnerabilități, amenințări sau măsuri de atenuare se primesc de ofițerul de securitate IT, se înregistrează, se evaluează fără întârziere în raport cu sistemele serviciului și, după caz, se transformă în măsuri, cu actualizarea GR-TSP; cele care privesc o criză în desfășurare se transmit echipei de management și acțiune în caz de urgență (REQ-7.11.3-02).

14.4. Copiile de siguranță și continuitatea

Copiile de siguranță și continuitatea respectă Politicile generale (cap. 12), Procedura DRP (PO_SI_63), Planul de continuitate a afacerii (PO_C_SI_S_63, cu Anexa 6) și secțiunea 6.11, cu următoarele precizări (ETSI EN 319 401, cl. 7.11):

– Planul de copii de siguranță stabilește, pentru fiecare sistem al serviciului: datele copiate, inclusiv datele de configurație ale sistemelor, ale echipamentelor de rețea și ale platformei de virtualizare; frecvența; legătura cu duratele de recuperare (RTO/RPO); locațiile (DC2, în afara rețelei sistemului copiat, și copia offline, păstrată separat de ambele centre de date); controalele fizice și logice, după clasa informațiilor (criptare pentru datele restricționate, acces numai pentru administratorii desemnați, jurnalizarea accesului); restaurarea (cererea, aprobarea Directorului Tehnic, verificarea după restaurare); duratele de păstrare ale copiilor, stabilite după cerințele de afaceri și cele legale. Datele serviciului și copiile lor se păstrează numai în centrele de date proprii și pe copia offline, fără servicii cloud ale terților. Planul se actualizează la fiecare modificare a sistemelor și cel puțin anual (REQ-7.11.2-01, REQ-7.11.2-02).

– Integritatea și completitudinea copiilor se verifică automat la fiecare copiere (sume de control, rapoartele de execuție) și la fiecare restaurare de probă; erorile generează alertă și se tratează ca incidente (REQ-7.11.2-03).

– Planul de continuitate al serviciului (Anexa 6 la PCA) se revizuiește cel puțin anual, după fiecare test sau activare a centrului de date secundar, după incidentele semnificative și la modificările semnificative ale serviciului, ale operațiunilor sau ale riscurilor (REQ-7.11.3-03, REQ-7.11.3-04).

14.5. Lanțul de aprovizionare

Politica de securitate a lanțului de aprovizionare, comună serviciilor de încredere CERTDIGITAL și aplicată serviciului, este următoarea (ETSI EN 319 401, cl. 7.14; ETSI TS 119 471, REQ-EAASP-7.14-01):

– **Domeniul și rolul**: politica guvernează relațiile cu furnizorii direcți și cu prestatorii de servicii care livrează produse, servicii sau procese TIC pentru serviciu (producătorii și distribuitorii modulelor criptografice, furnizorii platformei și ai componentelor software, furnizorii de conectivitate, de e-mail și de SMS, mentenanța echipamentelor și a clădirilor, colaboratorii externi), pentru a reduce riscurile identificate în GR-TSP (art. 21 alin. (2) lit. (d) din Directiva (UE) 2022/2555). Rolul CERTDIGITAL în lanțul de aprovizionare este cel de client și integrator al produselor și serviciilor TIC, care prestează serviciul în propriile centre de date și răspunde, în ansamblu, de conformitatea lui; CERTDIGITAL nu deleagă terților operarea serviciului, verificarea identității sau a atributelor ori gestionarea cheilor. Rolul se comunică fiecărui furnizor direct prin contract (REQ-7.14.1-01, REQ-7.14.1-03).

– **Selecția și contractarea**: înainte de contractare, furnizorii se evaluează conform procedurii interne PO_C_SI_S_24, după criteriile: a) practicile de securitate cibernetică ale furnizorului, inclusiv procedurile de dezvoltare securizată; b) capacitatea de a respecta specificațiile de securitate cibernetică, riscurile și nivelurile de clasificare ale serviciilor, sistemelor sau produselor livrate; c) calitatea și reziliența produselor și serviciilor TIC și măsurile de gestionare a riscurilor de securitate cibernetică încorporate în ele, inclusiv certificările (pentru modulele criptografice: Common Criteria EAL4+ sau EUCC și calificarea ca dispozitiv calificat); d) posibilitatea de a diversifica sursele de aprovizionare și de a limita dependența de un singur furnizor; e) rezultatele evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate ale lanțurilor de aprovizionare critice, unde există. Respectarea politicilor și a cerințelor de securitate ale CERTDIGITAL face parte din criteriile de selecție. Cerințele de securitate pentru achiziția produselor și serviciilor TIC se stabilesc înaintea achiziției, pe baza evaluării riscurilor (REQ-7.14.1-02, REQ-7.14.1-04, REQ-7.14.2-02, REQ-7.14.3-08).

– **Cerințele contractuale**: contractele și, unde este cazul, acordurile de nivel de serviciu cu furnizorii direcți cuprind, după caz: a) cerințele de securitate cibernetică, inclusiv pentru achiziția serviciilor și produselor TIC; b) cerințele privind instruirea, competențele și, unde este cazul, certificările personalului furnizorului; c) verificarea antecedentelor personalului furnizorului care are acces la sisteme sau la informații; d) obligația de a notifica CERTDIGITAL fără întârziere, în cel mult 24 de ore, incidentele care prezintă un risc pentru securitatea rețelelor și a sistemelor CERTDIGITAL, precum și canalul de raportare al CERTDIGITAL; e) dreptul de audit sau dreptul de a primi rapoartele de audit; f) obligația de a trata vulnerabilitățile care prezintă un risc pentru securitatea CERTDIGITAL; g) subcontractarea numai cu acordul CERTDIGITAL, cu transmiterea acelorași cerințe de

securitate subcontractanților; h) obligațiile la încetarea contractului, inclusiv returnarea sau distrugerea informațiilor obținute, cu proces-verbal; i) răspunderea furnizorului și obligația lui de a aplica controalele cerute de CERTDIGITAL; j) pentru produse: informațiile despre componentele software folosite, despre funcțiile de securitate implementate și despre configurația necesară funcționării în siguranță, precum și obligația furnizorului de a aplica practici de securitate adecvate față de propriii furnizori. Furnizorii care au acces la sisteme respectă planul de securitate și procedura de acces al terților (PO_SI_50); accesul în zonele de securitate se face numai însoțit, conform secțiunii 2.3 din Politica de securitate fizică și de mediu (REQ-7.14.2-03 – REQ-7.14.2-06, REQ-7.14.3-02, REQ-7.14.3-04, REQ-7.14.3-07, REQ-7.14.3-09, REQ-7.14.3-13).

– **Recepția, validarea și ciclul de viață**: componentele critice pentru funcționarea serviciului (modulele criptografice, serverele platformei, echipamentele de rețea și de securitate, aplicațiile serviciului) se identifică în inventarul activelor și în fișa serviciului din Anexa 6 la PCA. Echipamentele critice se achiziționează direct de la producător sau de la distribuitori autorizați; la recepție se verifică ambalajul și sigiliile, numerele de serie și versiunea de firmware sau suma de control a software-ului, cu proces-verbal, iar pentru modulele criptografice seria, firmware-ul și modul de operare se consemnează și la fiecare ceremonie (Procedura privind generarea cheilor, cap. 4 și anexa B). Programele și bibliotecile se obțin din surse verificate, cu verificarea semnăturii sau a sumei de control, iar lista componentelor software se ține pentru fiecare aplicație. Înainte de punerea în producție, produsele se testează în mediul de test pentru funcționarea conform specificației și pentru absența funcțiilor neașteptate sau nedorite; conformitatea cu cerințele de securitate se validează prin verificarea certificărilor, prin scanări de vulnerabilități și prin teste de penetrare. Pentru fiecare componentă se urmăresc versiunea, suportul producătorului și data sfârșitului suportului; înlocuirea se planifică înaintea sfârșitului suportului, iar riscurile componentelor învechite se tratează în GR-TSP (REQ-7.14.2-07 – REQ-7.14.2-11, REQ-7.14.2-13).

– **Monitorizarea și revizuirea**: furnizorii critici se evaluează cel puțin anual și după orice incident legat de produsele sau serviciile lor: rapoartele privind nivelul de serviciu, incidentele și vulnerabilitățile raportate, modificările practicilor lor de securitate cibernetică și ale produselor sau serviciilor livrate. Ofițerul de securitate IT stabilește nevoia unei evaluări neprogramate, iar constatările se consemnează. Riscurile rezultate din modificări se analizează și, unde este cazul, se iau fără întârziere măsuri de atenuare. Politica se revizuiește cel puțin anual, după incidente semnificative legate de furnizori și la modificări semnificative ale operațiunilor sau ale riscurilor (REQ-7.14.1-05, REQ-7.14.1-06, REQ-7.14.2-14, REQ-7.14.3-10).

– **Registrul furnizorilor**: ofițerul de securitate IT ține registrul furnizorilor direcți și al contractelor lor, cu: datele de contact ale fiecărui furnizor; produsele, serviciile și procesele

TIC furnizate; contractul și clauzele de securitate; locul în care furnizorul prelucrează, gestionează sau arhivează informații ale CERTDIGITAL; încadrarea ca furnizor critic. Registrul se revizuiește și se validează cel puțin anual, pentru a verifica valabilitatea și adecvarea contractelor și existența clauzelor de securitate (REQ-7.14.3-11, REQ-7.14.3-12, REQ-7.14.3-14).

– **Schimbul de informații**: informațiile despre problemele, vulnerabilitățile și compromiterile din lanțul de aprovizionare se schimbă cu furnizorii numai pe canalele stabilite prin contract, cu respectarea clasificării informațiilor (Politicile generale, secțiunea 4.2); ofițerul de securitate IT este punctul de contact al CERTDIGITAL (REQ-7.14.2-12).

– **Serviciile cloud**: componentele serviciului, datele lui și copiile de siguranță se găzduiesc numai în centrele de date proprii ale CERTDIGITAL. Serviciile cloud ale terților se folosesc numai pentru activități-suport (de exemplu, e-mailul domeniului principal), după evaluarea riscurilor și cu aprobarea ofițerului de securitate IT, cu împărțirea responsabilităților de securitate stabilită prin contract și fără date restricționate ale serviciilor de încredere. Regula este publică prin prezentul document (REQ-7.14.2-15).

– **Componentele furnizate de alte părți și responsabilitatea**: când serviciul folosește o componentă de serviciu de încredere furnizată de o altă parte, CERTDIGITAL folosește interfața componentei conform cerințelor furnizorului ei și verifică faptul că securitatea și funcționalitatea componentei corespund politicii și practicilor serviciului. CERTDIGITAL rămâne responsabil, în ansamblu, de conformitatea cu prezenta politică, cu politica de securitate a informației și cu politica serviciului (REQ-7.14.3-01, REQ-7.14.3-05, REQ-7.14.3-06).

– **Începerea și încetarea utilizării**: la începerea utilizării unui produs sau serviciu al unui furnizor se fac evaluarea, contractul, recepția și testarea, înscrierea în registru și acordarea accesului (PO_SI_50); la încetare se revocă accesul furnizorului, furnizorul returnează sau distruge informațiile CERTDIGITAL, cu proces-verbal, suporturile scoase din uz se șterg securizat, iar registrul se actualizează (REQ-7.14.3-03).

14.6. Verificarea configurației

Configurația sistemelor serviciului se verifică față de configurația de referință aprobată, automat, cel puțin o dată la 24 de ore, și manual, cel puțin o dată pe lună; intervalul maxim între două verificări este de 24 de ore, respectiv de o lună. Verificarea manuală cuprinde și setările de securitate, robustețea parolelor și activitățile efectuate cu conturile privilegiate, iar abaterile se tratează ca incidente de securitate (ETSI EN 319 401, REQ-6.3-08, REQ-6.3-09, REQ-7.7-10).

14.7. Organizațiile externe care susțin serviciul

Organizațiile externe care susțin serviciul și obligațiile lor sunt (ETSI EN 319 401, REQ-6.1-04):

– **furnizorul platformei de emitere și al componentelor software**, înscris în registrul furnizorilor critici: livrează actualizările de securitate și suportul în termenele din contract, accesează sistemul numai conform procedurii de acces al terților, însoțit, și nu are acces la cheia sigiliului, la datele titularilor sau la listele de stare;

– **Thales**, producătorul modulelor Luna PCIe HSM 7: furnizează firmware-ul, suportul și menținerea certificărilor modulelor (dispozitiv calificat de creare a sigiliului, Common Criteria, FIPS 140-3);

– **RCS & RDS și Orange Romania Communications**: asigură conectivitatea redundantă a centrelor de date, conform contractelor de nivel de serviciu;

– **sursele autentice** (de exemplu, ONRC) și mecanismul național de verificare a atributelor: răspund cererilor de verificare a atributelor în condițiile proprii;

– **Comisia Europeană și furnizorii de portofele**: publică listele de încredere ale furnizorilor de portofele și informațiile de revocare a unităților de portofel;

– **organismul de înregistrare și autoritatea care emite certificatele de acces** (RE 2025/848, modificat prin RE 2026/1730): înregistrează CERTDIGITAL ca parte care se bazează pe portofel și emit certificatul de acces.

Obligațiile contractuale de securitate și de confidențialitate ale furnizorilor sunt cele din secțiunea 14.5, iar furnizorii critici se evaluează cel puțin anual. CERTDIGITAL rămâne responsabil, în ansamblu, de prestarea serviciului.

15. Aspecte juridice și comerciale

Obligațiile solicitantului, ale subiectului și ale titularului (cuprinse și în termenii și condițiile serviciului, conform REQ-EAASP-4.2.3.1-01) sunt:

– să furnizeze informații corecte și complete;

– să protejeze portofelul;

– să ceară revocarea când atributele nu mai sunt corecte sau portofelul a fost compromis;

– să folosească atestatele numai pe durata valabilității lor, în scopuri legale și în limitele notificate prin prezentul document și prin termenii și condițiile serviciului;

– să nu folosească și să nu permită folosirea neautorizată a atestatelor.

Tarifele, răspunderea (art. 13 din Regulamentul eIDAS), asigurarea, modificările, soluționarea litigiilor și legea aplicabilă sunt cele din capitolele 7 și 8 și din termenii și condițiile serviciului.

Anexa A – Politicile atestatelor

A.1. Reprezentantul legal al persoanei juridice (OID 1.3.6.1.4.1.47898.15.1.1)

Element	Regula
Scopul	dovedește că o persoană fizică este înscrisă ca reprezentant legal al unei persoane juridice și modul în care o reprezintă (anexa VI pct. 9)
Subiectul și titularul	persoana fizică reprezentant legal; atestatul se emite în portofelul ei
Atributele	numele și prenumele; calitatea (de exemplu, administrator); modul de exercitare a reprezentării (singur sau împreună) și limitele înscrise; denumirea, EUID și codul unic de înregistrare ale persoanei juridice; data informației din registru
Sursa și metoda	registrul comerțului (ONRC), prin informații obținute electronic de la ONRC, iar după punerea lui în funcțiune, prin mecanismul național de verificare (art. 24 alin. (1b) lit. (d); art. 45e). Subiectul se identifică în registru pe baza datelor de identificare verificate conform secțiunii 6.4; codul numeric personal nu se înscrie în atestat
Nivelul de asigurare a identității	ridicat; identitatea solicitantului se verifică prin una dintre metodele de la art. 24 alin. (1a) din Regulamentul eIDAS (secțiunile 6.4 și 12.2)
Formatele	SD-JWT VC (ETSI TS 119 472-1, clauza 5) și mdoc (ISO/IEC 18013-5; ETSI TS 119 472-1, clauza 6); ambele formate se oferă
Schema atributelor	anexa C.1 (numele revendicărilor, identificatorii elementelor mdoc, tipurile și codificarea)
Mecanismele de probă	sigiliul electronic calificat al CERTDIGITAL, JAdES pentru SD-JWT VC și COSE pentru mdoc, cu cheia CERTDIGITAL QEAA SERVICE G5 (ES256); fiecare atribut este divulgabil selectiv (secțiunea 12.4)
Legarea de portofel	obligatorie: atestatul se leagă criptografic de o cheie a aplicației criptografice securizate a portofelului (WSCA) din unitatea de portofel a titularului (`cnf` / `deviceKeyInfo`), cu dovada posesiei la emitere și cu verificarea atestatului cheilor; dispozitivul criptografic securizat al portofelului (WSCD) trebuie să aibă nivelul de securitate corespunzător nivelului de asigurare ridicat – rezistență la atacatori cu potențial de atac ridicat (ISO/IEC 18045, AVA_VAN.5) –, dovedit prin atestatul cheilor emis de furnizorul portofelului și prin certificarea soluției de portofel; dacă nivelul nu este dovedit, atestatul nu se emite (ETSI TS 119 471, REQ-EAASP-4.2.1.2-03, REQ-EAASP-4.2.2.3-04, -06; secțiunile 11.3 și 12.5)
Minimizarea datelor	setul de atribute este cel minim necesar scopului atestatului; codul numeric personal se folosește numai pentru comparația cu registrul și nu se înscrie în atestat (ETSI TS 119 471, REQ-EAASP-7.13-04)
Valabilitatea și starea	cel mult 12 luni, cu listă de stare și reverificare zilnică la sursă; valabilitatea maximă este stabilită ținând seama de cerințele de securitate (reverificarea zilnică la sursă, revocarea în cel mult 24 de ore) și de riscul de urmărire a titularului (loturi de unică folosință, poziții aleatorii în liste de stare) (ETSI TS 119 471, REQ-EAASP-4.2.2.3-18); atestatul nu se emite ca atestat de scurtă durată și poate fi revocat atât la cerere, cât și din inițiativa CERTDIGITAL (secțiunea 12.6)
Revocarea specifică	încetarea sau modificarea calității ori a modului de reprezentare în registrul comerțului; radierea sau dizolvarea persoanei juridice; cererea persoanei juridice reprezentate (secțiunea 6.3.1)
Cadrul de încredere	Lista de încredere a României, în care serviciul se înscrie cu tipul `EAA/Q` (secțiunea 1.2); listele de încredere ale furnizorilor de portofele, publicate de Comisie; sistemul de atestare de mai jos

Element	Regula
Sistemul de atestare	sistemul de atestare propriu CERTDIGITAL, versiunea 1, definit în prezenta anexă și în anexa C pentru tipurile A.1 și A.2; tipul A.1: vct `https://eaa.certdigital.ro/vct/legal-representative/1` (SD-JWT VC) și docType `ro.certdigital.eaa.legal_representative.1` (mdoc). CERTDIGITAL, ca proprietar al sistemului, solicită înregistrarea lui în catalogul sistemelor de atestare a atributelor (art. 8 alin. (3) din RE 2025/1569); atestatele emise în cadrul unui sistem înregistrat în catalog respectă cerințele acelui sistem (art. 3 alin. (2) din RE 2025/1569)

A.2. Datele de identificare ale persoanei juridice (OID 1.3.6.1.4.1.47898.15.1.2)

Element	Regula
Scopul	dovedește datele de identificare ale unei persoane juridice înscrise în registrul comerțului (anexa VI pct. 11)
Subiectul și titularul	persoana juridică; atestatul se emite în portofelul persoanei juridice sau al reprezentantului ei legal, după verificarea calității acestuia (A.1); reprezentantul legal deține atestatul și îl prezintă numai în numele persoanei juridice (excepția de la controlul exclusiv al subiectului, stabilită la secțiunea 6.3.1)
Atributele	denumirea; forma juridică; EUID; numărul de ordine în registrul comerțului; codul unic de înregistrare; sediul; starea (de exemplu, activă); data înregistrării; data informației din registru
Sursa și metoda	registrul comerțului (ONRC), ca la A.1
Nivelul de asigurare a identității	ridicat; identitatea solicitantului se verifică prin una dintre metodele de la art. 24 alin. (1a) din Regulamentul eIDAS (secțiunile 6.4 și 12.2), iar calitatea lui de reprezentant legal se verifică în registrul comerțului (A.1)
Formatele	SD-JWT VC (ETSI TS 119 472-1, clauza 5) și mdoc (ISO/IEC 18013-5; ETSI TS 119 472-1, clauza 6); ambele formate se oferă
Schema atributelor	anexa C.2 (numele revendicărilor, identificatorii elementelor mdoc, tipurile și codificarea)
Mecanismele de probă	ca la A.1
Legarea de portofel	obligatorie, ca la A.1: atestatul se leagă criptografic de o cheie a WSCA din unitatea de portofel a titularului (`cnf` / `deviceKeyInfo`), cu dovada posesiei la emitere și cu verificarea atestatului cheilor; nivelul de securitate cerut pentru dispozitivul criptografic securizat al portofelului (WSCD) este cel de la A.1 (ETSI TS 119 471, REQ-EAASP-4.2.1.2-03, REQ-EAASP-4.2.2.3-04, -06)
Minimizarea datelor	setul de atribute este cel minim necesar identificării persoanei juridice; atestatul nu conține date cu caracter personal ale reprezentanților (ETSI TS 119 471, REQ-EAASP-7.13-04)
Valabilitatea și starea	cel mult 12 luni, cu listă de stare și reverificare zilnică la sursă; valabilitatea maximă este stabilită ca la A.1 (ETSI TS 119 471, REQ-EAASP-4.2.2.3-18); atestatul nu se emite ca atestat de scurtă durată și poate fi revocat atât la cerere, cât și din inițiativa CERTDIGITAL (secțiunea 12.6)
Revocarea specifică	modificarea în registru a oricărui atribut atestat; radierea, dizolvarea sau intrarea în insolvență, dacă afectează starea atestată; încetarea calității de reprezentant legal a titularului care deține atestatul în numele persoanei juridice (secțiunea 6.3.1)
Cadrul de încredere	ca la A.1
Sistemul de atestare	sistemul de atestare propriu CERTDIGITAL, ca la A.1; tipul A.2: vct `https://eaa.certdigital.ro/vct/legal-person/1` (SD-JWT VC) și docType `ro.certdigital.eaa.legal_person.1` (mdoc)

Anexa B – Corespondența practicilor (Partea a II-a) cu cerințele

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 24 alin. (1a), (1b)	metodele de verificare a identității și a atributelor	12.2, 12.3
art. 45d alin. (4); RE 2025/1569, art. 4	revocarea definitivă; numai prestatorul revocă; trasabilitate împiedicată; integritatea informațiilor de stare	12.6, 13.2
art. 45e; RE 2025/1569, art. 9; TS 119 478	verificarea la sursele autentice	12.3
art. 45g	interfața cu portofelele	11
art. 45h	separarea datelor și a funcțiilor	13.1
anexa V lit. (a)–(i)	conținutul atestatului	12.4
ETSI TS 119 471 V1.1.1 (adaptat prin RE 2026/1735)	cerințele pentru prestator	10–15
REQ-EAASP-6.1.1-01 (ETSI EN 319 401, cl. 6.1)	politica și declarația de practici; corespondența cu documentele prevăzute de ETSI TS 119 471	1.2
REQ-EAASP-4.2.2.1-09	emiterea conform politicii serviciului și politicii atestatului	6.6, 12.4, anexa A
REQ-EAASP-4.2.2.3-02, -03	certificat de acces; validarea unității de portofel	11.2, 11.3
REQ-EAASP-4.2.2.3-06	legarea de portofel, obligatorie pentru toate tipurile de atestat	12.5, anexa A
REQ-EAASP-4.2.3.1-01	obligațiile subiectului, cuprinse în declarația de practici și în termenii și condițiile serviciului	15
REQ-EAASP-4.2.3.1-02	controlul exclusiv al subiectului; excepțiile stabilite de politică (A.2 și contractul-cadru)	6.3.1, anexa A.2
REQ-EAAS-4.2.4.1-01; REQ-EAASP-4.2.4.1-02	reînnoirea: procesul, verificarea valabilității atestatului și a informațiilor folosite la verificare	12.5
REQ-EAASP-4.2.5.1-04	nu există atestate care să nu poată fi revocate prin serviciul de revocare sau din inițiativa CERTDIGITAL	12.6
REQ-EAASP-4.2.5.2-05; REQ-EAASP-4.2.5.2-06	informațiile de revocare sunt incluse în toate atestatele; nu se emit atestate de scurtă durată	12.6
REQ-EAASP-6.1-02	mecanismul de revocare	12.6
REQ-EAASP-6.1.2-01	riscul de corelare de către prestator; nicio colaborare cu părțile care se bazează pentru urmărirea titularilor	13.2
REQ-EAASP-7.10-02 – 7.10-07; REQ-EAASP-7.10-08	informațiile înregistrate și accesul la ele; duratele de păstrare și informațiile care se predau la încetare	13.3
REQ-EAASP-7.13-04	minimizarea datelor în politica fiecărui atestat	anexa A, anexa C
REQ-EAASP-7.5.3-01A, -01B, -02	agilitate criptografică; ECCG ACM; sigiliul pe dispozitiv calificat	14
REQ-EAASP-7.9-02; REQ-EAASP-7.12-04	monitorizarea; planul de încetare	14
ETSI TS 119 472-1 V1.2.1, cl. 5–6 (adaptat prin RE 2026/1731)	formatele SD-JWT VC și mdoc; schema atributelor; stare fără suspendare; nu se emit atestate de scurtă durată	12.4, 12.6, anexa C
ETSI TS 119 472-3 V1.1.1	protocolul de emitere	11.1
RE 2025/848, modificat prin RE 2026/1730	înregistrarea ca parte care se bazează pe portofel	11.2
RE 2025/1566 (TS 119 461 V2.1.1)	verificarea identității, din 19.08.2027	12.2

Anexa C – Schema atributelor

Prezenta anexă stabilește schema atributelor pentru fiecare tip de atestat din anexa A (ETSI TS 119 471, clauza 6.4): numele revendicării în formatul SD-JWT VC și identificatorul elementului de date în formatul mdoc, tipul de date și codificarea, caracterul obligatoriu și divulgarea selectivă. Se aplică următoarele reguli comune:

– identificatorul elementului de date mdoc este identic cu numele revendicării SD-JWT VC; elementele de date mdoc se află în spațiul de nume indicat pentru fiecare tip de atestat;

– valorile de tip text sunt șiruri de caractere codificate UTF-8 (în mdoc, tipul CBOR `tstr`), preluate din registrul comerțului fără transliterare, cu diacriticele limbii române;

– datele calendaristice au formatul `full-date` din ISO 8601 (AAAA-LL-ZZ); în mdoc, valoarea `full-date` se codifică cu eticheta CBOR 1004 (RFC 8943);

– toate atributele din tabele sunt divulgabile selectiv: în SD-JWT VC, fiecare revendicare are propria dezvăluire (disclosure); în mdoc, fiecare element de date are propriul rezumat în obiectul de securitate (MSO);

– elementele de structură ale atestatului (emitentul, tipul, valabilitatea, referința de stare, cheia de legare și mențiunea de atestat calificat, secțiunea 12.4) nu sunt divulgabile selectiv și sunt prezente în orice prezentare;

– un atribut opțional lipsește din atestat când informația nu este înscrisă în registru; CERTDIGITAL nu înscrie în atestat valori goale.

Schema se publică și ca metadate ale tipului, la adresa vct indicată în anexa A. Orice modificare a schemei se face printr-o versiune nouă a tipului de atestat, cu vct și docType noi, și printr-o versiune nouă a prezentului document (secțiunea 5.3).

C.1. Reprezentantul legal al persoanei juridice (A.1)

Spațiul de nume mdoc este `ro.certdigital.eaa.legal_representative.1`.

Atributul	Revendicarea SD-JWT VC / elementul mdoc	Tipul și codificarea	Obligatoriu / divulgabil selectiv
numele	`family_name`	șir de caractere UTF-8, ca în registrul comerțului	obligatoriu; divulgabil selectiv
prenumele	`given_name`	șir de caractere UTF-8, ca în registrul comerțului	obligatoriu; divulgabil selectiv
calitatea	`representative_role`	șir de caractere UTF-8: denumirea calității din registrul comerțului (de exemplu, „administrator”)	obligatoriu; divulgabil selectiv
modul de exercitare a reprezentării	`representation_mode`	șir de caractere UTF-8, cu una dintre valorile `individual` (singur) sau `joint` (împreună)	obligatoriu; divulgabil selectiv

Atributul	Revendicarea SD-JWT VC / elementul mdoc	Tipul și codificarea	Obligatoriu / divulgabil selectiv
limitele înscrise ale reprezentării	`representation_limits`	șir de caractere UTF-8: textul limitelor înscrise în registrul comerțului	opțional, prezent numai dacă în registru sunt înscrise limite; divulgabil selectiv
denumirea persoanei juridice	`legal_person_name`	șir de caractere UTF-8, ca în registrul comerțului	obligatoriu; divulgabil selectiv
EUID-ul persoanei juridice	`legal_person_euid`	șir de caractere UTF-8: identificatorul unic european (de exemplu, `ROONRC.J1991000103187`)	obligatoriu; divulgabil selectiv
codul unic de înregistrare al persoanei juridice	`legal_person_cui`	șir de caractere UTF-8: numai cifrele codului, fără atributul fiscal „RO”	obligatoriu; divulgabil selectiv
data informației din registru	`register_information_date`	`full-date` ISO 8601	obligatoriu; divulgabil selectiv

C.2. Datele de identificare ale persoanei juridice (A.2)

Spațiul de nume mdoc este `ro.certdigital.eaa.legal_person.1`.

Atributul	Revendicarea SD-JWT VC / elementul mdoc	Tipul și codificarea	Obligatoriu / divulgabil selectiv
denumirea	`legal_person_name`	șir de caractere UTF-8, ca în registrul comerțului	obligatoriu; divulgabil selectiv
forma juridică	`legal_form`	șir de caractere UTF-8: forma juridică din registrul comerțului (de exemplu, „societate pe acțiuni”)	obligatoriu; divulgabil selectiv
EUID	`legal_person_euid`	șir de caractere UTF-8: identificatorul unic european (de exemplu, `ROONRC.J1991000103187`)	obligatoriu; divulgabil selectiv
numărul de ordine în registrul comerțului	`trade_register_number`	șir de caractere UTF-8 (de exemplu, `J1991000103187`)	obligatoriu; divulgabil selectiv
codul unic de înregistrare	`legal_person_cui`	șir de caractere UTF-8: numai cifrele codului, fără atributul fiscal „RO”	obligatoriu; divulgabil selectiv
sediul	`registered_office`	șir de caractere UTF-8: adresa sediului social, ca în registrul comerțului	obligatoriu; divulgabil selectiv
starea	`legal_status`	șir de caractere UTF-8: starea din registrul comerțului (de exemplu, „activă”)	obligatoriu; divulgabil selectiv
data înregistrării	`registration_date`	`full-date` ISO 8601	obligatoriu; divulgabil selectiv
data informației din registru	`register_information_date`	`full-date` ISO 8601	obligatoriu; divulgabil selectiv