

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

Cuprins

PARTEA I – Politica serviciului 7
1. Introducere 7
1.1. Prezentare generală 7
1.2. Identificarea documentului și a politicilor 7
1.3. Participanții și furnizorii externi 8
1.4. Utilizarea serviciului și efectele juridice 9
1.5. Administrarea documentului 9
2. Referințe normative 10
2.1. Acte normative și standarde 10
3. Definiții și acronime 12
3.1. Definiții 12
3.2. Acronime 12
4. Concepte generale 14
4.1. Serviciul și componentele sale 14
4.2. Interfața cu portofelele europene pentru identitatea digitală 14
4.3. Formatele atestatelor 14
4.4. Politicile atestatelor 14
4.5. Identitatea serviciului și sigiliul serviciului 15
5. Politica serviciului 16
5.1. Identificare și conformitate 16
5.2. Comunitatea utilizatorilor și aplicabilitatea 16
5.3. Modificarea politicii 16
6. Cerințele privind practicile 17
6.1. Publicare și depozit 17
6.2. Termeni și condiții 17
6.3. Cererea de emitere 17
6.4. Verificarea identității 17
6.5. Verificarea atributelor 17
6.6. Emiterea atestatului 18
6.7. Valabilitatea, starea și revocarea 18

6.8. Separarea serviciului și protecția vieții private 19
6.9. Timpul de încredere și jurnalele 19
6.10. Personalul 20
6.11. Controale privind facilitățile, managementul și operarea 20
6.12. Controale criptografice și de rețea 20
6.13. Notificări către ADR și încetarea serviciului 21
6.14. Evaluarea conformității 21
7. Obligații și răspundere 22
7.1. Obligațiile CERTDIGITAL 22
7.2. Obligațiile solicitantului, ale subiectului și ale titularului 22
7.3. Obligațiile părților care se bazează 22
7.4. Răspunderea 22
7.5. Asigurarea 23
8. Alte aspecte comerciale și juridice 24
8.1. Tarife 24
8.2. Protecția datelor cu caracter personal 24
8.3. Modificări 24
8.4. Soluționarea litigiilor 24
8.5. Legea aplicabilă și cadrul legal 24
8.6. Alte prevederi 25
9. Corespondența cu cerințele Regulamentului eIDAS și ale regulamentelor de punere în aplicare 26
9.1. Tabel de corespondență 26
PARTEA A II-A – Declarația de practici 27
10. Publicare și depozit 27
11. Interfața cu portofelele 28
11.1. Fluxul de emitere 28
11.2. Autentificarea reciprocă și înregistrarea 28
11.3. Validarea unității de portofel 28
11.4. Limite 29
12. Ciclul de viață al atestatului 30
12.1. Cererea 30
12.2. Verificarea identității 30
12.3. Verificarea atributelor 30

12.4. Emiterea și conținutul atestatului 31
12.5. Legarea de titular, loturile și reemiterea 31
12.6. Revocarea și informațiile de stare 31
13. Datele, separarea și păstrarea 33
13.1. Separarea serviciului (art. 45h) 33
13.2. Riscul de corelare 33
13.3. Durata păstrării 33
13.4. Protecția datelor 33
14. Controale de management și operare 34
15. Aspecte juridice și comerciale 35
Anexa A – Politicile atestatelor 36
A.1. Reprezentantul legal al persoanei juridice (OID 1.3.6.1.4.1.47898.15.1.1) 36
A.2. Datele de identificare ale persoanei juridice (OID 1.3.6.1.4.1.47898.15.1.2) 36
Anexa B – Corespondența practicilor (Partea a II-a) cu cerințele 37

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 sau 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. El este prestat ca serviciu calificat, înscris în Lista de încredere a României cu tipul `EAA/Q`.

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. Pentru cerințele comune tuturor serviciilor se aplică Politicile generale CertDigital (PG, v2.0).

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	1.0
Data	22.10.2026
Identificator (OID)	1.3.6.1.4.1.47898.15.1 – prezentul document (politica serviciului și declarația de practici)
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)

Element	Valoare
Declarația de practici	declarația de practici este inclusă în prezentul document (Partea a II-a); identificatorul 1.3.6.1.4.1.47898.15.2, 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	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).

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, dacă sunt supuse revocării, 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. 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).

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 de cel mult 24 de ore, care nu este supus revocării;

– **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
QEAA	atestat electronic calificat al atributelor

Acronim	Semnificație
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. Formatele oferite pentru fiecare tip de atestat sunt stabilite în politica lui (anexa A).

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 identifică serviciul în Lista de încredere:

– 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 cheia ECDSA P-256 generată în ceremonia cheilor G5 din 23.10.2026, în modulul Thales Luna PCIe HSM 7 A790 (secțiunea 14). Profilul lui este descris în DPC CERTDIGITAL G5, secțiunea 7.1.2, iar certificatul se publică la http://certs.certdigital.ro/certdigital_qeaa_g5.crt.

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). Serviciul este prestat ca serviciu calificat, înscris în Lista de încredere (art. 21).

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.

6.4. 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

– 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 și, pentru atestatele supuse revocării, adresa listei de stare și poziția atestatului în listă;

– 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 de o cheie a unității de portofel a titularului, a cărei posesie se verifică la emitere; 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

– **atestatele de scurtă durată** (valabilitate de cel mult 24 de ore) nu sunt supuse revocării; tipurile de atestat de scurtă durată sunt enumerate în secțiunea 12.6;

– **atestatele cu valabilitate mai mare de 24 de ore** 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; unitatea de portofel a fost revocată sau cheia titularului a fost compromisă; subiectul a decedat sau a fost radiat;

– revocarea se efectuează în cel mult 24 de ore de la primirea cererii sau de la luarea la cunoștință a motivului; când un atestat face parte dintr-un lot, se revocă întregul lot; titularul este informat; 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;

– 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 (v2.0), 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;

– 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;

– 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 și evidențele se transferă entității desemnate, iar datele serviciului, păstrate separat (art. 45h), se transferă sau 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.

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 (pentru atestatele supuse revocării) 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/ce-este-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; atestatele 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-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. 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 conțin 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;

– faptul că unitatea de portofel și cheile ei nu au fost revocate și că cheile se află în dispozitivul securizat al portofelului, la nivelul cerut de politica atestatului.

Pentru atestatele valabile mai mult de 24 de ore, CERTDIGITAL verifică cel puțin o dată la 24 de ore starea unității de portofel și a cheilor pe care sunt legate atestatele; dacă acestea au fost revocate, atestatele se revocă (secțiunea 12.6).

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

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.

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;

– pentru atestatele cu valabilitate mai mare de 24 de ore, atributele se reverifică la sursă zilnic; 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; pentru atestatele supuse revocării, referința `status` (adresa listei și poziția)	referința de stare din MSO (listă de stare sau listă de identificatori)
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.

12.5. Legarea de titular, loturile și reemiterea

– 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;

– un lot nou pentru aceleași atribute se poate emite în perioada de valabilitate inițială, după autentificarea titularului, fără prelungirea valabilității; prelungirea valabilității înseamnă o emitere nouă, cu verificarea atributelor la sursă.

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 sau a revocării unității de portofel; întregul lot se revocă; titularul este informat;

– **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** (cel mult 24 de ore) nu sunt supuse revocării și nu au referință de stare. Tipurile emise ca atestate de scurtă durată: varianta de scurtă durată a atestatului A.1, dacă este oferită.

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 este evaluat în analiza de risc a serviciului. Măsurile: 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.

13.3. Durata păstrării

Ce se păstrează	Cât
dovezile verificării identității și a atributelor	cel puțin 10 ani de la expirarea atestatului
evidența atestatelor emise (tipul, atributele, valabilitatea, poziția în lista de stare, cheia de legare) și a revocărilor	cel puțin 10 ani de la expirarea atestatului
jurnalele serviciului	cel puțin 10 ani
cererile respinse	1 an

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 (v2.0) 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;

– **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;

– **jurnalizarea**: cererile, verificările, emiterile, revocările, publicarea listelor de stare, operațiile administrative și evenimentele de securitate; 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;

– **încetarea**: conform planului 00r, anexa A14 (RE 2025/2530): listele de stare și evidențele se transferă entității desemnate, 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.

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
Formatele	SD-JWT VC; mdoc, dacă sistemul de atestare o cere
Valabilitatea și starea	cel mult 12 luni, cu listă de stare și reverificare zilnică la sursă; varianta de scurtă durată, de cel mult 24 de ore, fără stare
Revocarea specifică	încetarea sau modificarea calității ori a modului de reprezentare în registrul comerțului; radierea sau dizolvarea persoanei juridice
Sistemul de atestare	sistemul de atestare propriu CERTDIGITAL, versiunea 1, definit în prezenta anexă 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)
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
Formatele	SD-JWT VC; mdoc, dacă sistemul de atestare o cere
Valabilitatea și starea	cel mult 12 luni, cu listă de stare și reverificare zilnică la sursă
Revocarea specifică	modificarea în registru a oricărui atribut atestat; radierea, dizolvarea sau intrarea în insolvență, dacă afectează starea atestată
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-4.2.2.3-02, -03	certificat de acces; validarea unității de portofel	11.2, 11.3
REQ-EAASP-4.2.3.1-01	obligațiile subiectului, cuprinse în declarația de practici și în termenii și condițiile serviciului	15
REQ-EAASP-6.1-02	mecanismul de revocare	12.6
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; stare fără suspendare; atestatele de scurtă durată	12.4, 12.6
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