

Politica și declarația de practici a serviciului de păstrare calificată

CertDigital QPS

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	Director Tehnic	Versiunea inițială	27/08/2025
2.0	Ofițer de Securitate IT	Rescriere completă pentru eIDAS 2 (Reg. (UE) 2024/1183), în limba română, conform TS 119 511, TS 119 512 și Reg. (UE) 2025/1946: profiluri WOS/WST/WTS/PGD/AUG descrise formal (scheme și formate ETSI), perioada de grație de 24 de ore, augmentarea în trei etape, fără protocol de notificare, export și sfârșitul perioadei de păstrare; păstrare 10 ani; maximum 500 MB; RSA ≥ 3072; certificatul QPS G4; qps.certdigital.ro; TSA G4; GDPR art. 28; răspundere, asigurare, încetare; identificatorii rămân în arcul 1.3.6.1.4.1.47898.10, cu profilurile PGD și AUG adăugate (CERTDIGITAL_OID_MAP); temeiul publicării tarifelor: art. 11 alin. (1) din Legea nr. 214/2024	24/10/2026
2.1	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; începutul valabilității profilurilor rămâne data intrării în vigoare a versiunii 2.0	27/10/2026
2.2	Ofițer de Securitate IT	Trimiterile la celelalte documente CertDigital nu mai au număr de versiune: se aplică versiunea în vigoare, publicată la adresa fixă din depozit, iar versiunile anterioare sunt în arhivă	27/10/2026

Cuprins

1. Introducere 6
1.1. Prezentare generală 6
1.2. Identificarea documentului și a politicilor 6
1.3. Participanții 7
1.4. Relația cu alte documente 7
1.5. Administrarea documentului 7
1.6. Referințe normative 7
2. Definiții și acronime 9
2.1. Definiții 9
2.2. Acronime 9
3. Descrierea serviciului 10
3.1. Obiectivele de păstrare 10
3.2. Modelele de stocare 10
3.3. Formatele acceptate 10
3.4. Operațiile serviciului (ETSI TS 119 512) 11
3.5. Limitări 11
3.6. Profilurile de păstrare 11
4. Politicile serviciului 14
4.1. Politica de validare implicită (OID 1.3.6.1.4.1.47898.10.2.1) 14
4.2. Politica criptografică (OID 1.3.6.1.4.1.47898.10.3) 14
4.3. Politica privind formatul dovezilor (OID 1.3.6.1.4.1.47898.10.4) 15
4.4. Profilul API (OID 1.3.6.1.4.1.47898.10.5) 15
5. Practicile serviciului 16
5.1. Preluarea obiectelor 16
5.2. Generarea dovezilor 16
5.3. Augmentarea (reînnoirea) dovezilor 16
5.4. Protocolul de notificare 17
5.5. Regăsirea, validarea și accesul la obiecte 17
5.6. Exportul, ștergerea și sfârșitul perioadei de păstrare 17
5.7. Jurnale și trasabilitate 17

5.8. Gestionarea incidentelor 18
6. Mediul serviciului și controale 19
6.1. Controale generale 19
6.2. Securitatea fizică 19
6.3. Certificatul și cheia serviciului 19
6.4. Marcarea temporală 20
6.5. Sincronizarea timpului 20
6.6. Disponibilitate și continuitate 20
7. Obligații 21
7.1. Obligațiile CERTDIGITAL 21
7.2. Obligațiile abonatului 21
7.3. Obligațiile părții care se bazează 21
8. Răspundere și aspecte juridice 22
8.1. Răspunderea 22
8.2. Asigurarea 22
8.3. Protecția datelor cu caracter personal 22
8.4. Tarife 22
8.5. Soluționarea litigiilor 23
8.6. Legea aplicabilă și cadrul legal 23
8.7. Modificări 23
8.8. Încetarea serviciului 23
9. Evaluarea conformității 24

1. Introducere

1.1. Prezentare generală

Prezentul document este Politica și declarația de practici a serviciului de păstrare calificată (PSPPS) CERTDIGITAL QPS, operat de CENTRUL DE CALCUL S.A. (marca CertDigital, denumită în continuare „CERTDIGITAL”), prestator de servicii de încredere calificat. Documentul reunește politica și practicile serviciului, conform ETSI TS 119 511 V1.1.1.

Serviciul asigură păstrarea calificată a semnăturilor electronice calificate (art. 34 din Regulamentul (UE) nr. 910/2014) și a sigiliilor electronice calificate (art. 40), adică prelungirea fiabilității acestora dincolo de perioada de valabilitate tehnologică, prin dovezi de păstrare. Serviciul respectă Regulamentul de punere în aplicare (UE) 2025/1946, Regulamentul de punere în aplicare (UE) 2025/2530 și ETSI EN 319 401 V3.1.1.

Versiunea 2.0 înlocuiește versiunea inițială 1.0 (27.08.2025).

Pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României (art. 21 din Regulamentul (UE) nr. 910/2014); până la înscriere, serviciul nu se prestează ca serviciu de încredere calificat (art. 21 alin. (3)).

1.2. Identificarea documentului și a politicilor

OID	Denumire
1.3.6.1.4.1.47898.10.1	Politica și declarația de practici a serviciului de păstrare (prezentul document)
1.3.6.1.4.1.47898.10.1.1	Profil de păstrare WOS: fără stocare
1.3.6.1.4.1.47898.10.1.2	Profil de păstrare WST: cu stocare
1.3.6.1.4.1.47898.10.1.3	Profil de păstrare WTS: cu stocare temporară
1.3.6.1.4.1.47898.10.1.4	Profil PGD: păstrarea datelor generale (dovada existenței datelor)
1.3.6.1.4.1.47898.10.1.5	Profil AUG: augmentarea dovezilor de păstrare transmise
1.3.6.1.4.1.47898.10.2 / 10.2.1	Politica de validare a serviciului / politica de validare implicită
1.3.6.1.4.1.47898.10.3	Politica criptografică
1.3.6.1.4.1.47898.10.4	Politica privind formatul dovezilor
1.3.6.1.4.1.47898.10.5	Profilul API al serviciului

Identificatorii sunt înscriși în CERTDIGITAL_OID_MAP și apar în contracte, în obiectele și containerele de păstrare, în rapoartele de validare și în jurnale. În protocolul de păstrare (ETSI TS 119 512), profilurile se identifică prin URI-ul `urn:oid:1.3.6.1.4.1.47898.10.1.x` (secțiunea 3.6).

Identificatorii serviciului rămân în arcul 1.3.6.1.4.1.47898.10, ca în versiunea 1.0 (CERTDIGITAL_OID_MAP, secțiunea 10). Versiunea 2.0 adaugă identificatorii profilurilor PGD (1.3.6.1.4.1.47898.10.1.4) și AUG (1.3.6.1.4.1.47898.10.1.5). Identificatorul 1.3.6.1.4.1.47898.10.6,

menționat în versiunea 1.0 pentru o eventuală includere a profilului PGD, nu a fost alocat și rămâne rezervat.

1.3. Participanții

– **prestatorul**: CENTRUL DE CALCUL S.A., care operează serviciul și răspunde de el;

– **abonatul**: persoana fizică sau juridică ce a încheiat contract pentru utilizarea serviciului și transmite obiecte spre păstrare;

– **partea care se bazează**: persoana care se bazează pe o dovadă de păstrare emisă de CERTDIGITAL;

– **ADR**, organism de supraveghere, și **organismul de evaluare a conformității**.

Serviciul utilizează exclusiv componente proprii ale CERTDIGITAL, inclusiv serviciul de marcare temporală calificată CERTDIGITAL TSA G4; nu se utilizează furnizori externi pentru funcțiile serviciului.

1.4. Relația cu alte documente

Se aplică, în completare: Politicile generale CertDigital, Termenii și condițiile serviciului (TC-QPS), contractul serviciului (CTR-QPS), Politica de protecție a datelor (00d), Procedura de notificare a incidentelor (00q), Procedura de continuitate operațională (PO/SI/63) și Planul de încetare (00r).

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, inclusiv politicile de validare, criptografică și privind dovezile pe care le conține, este redactat în limba română. În caz de neconcordanță cu o traducere, prevalează versiunea în limba română.

1.6. Referințe normative

– Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183, art. 34 și 40;

– Regulamentul de punere în aplicare (UE) 2025/1946 (păstrarea calificată a semnăturilor și sigiliilor electronice calificate) și Regulamentul de punere în aplicare (UE) 2025/2530;

– ETSI TS 119 511 V1.1.1 (cerințe de politică și securitate pentru prestatorii de servicii de păstrare);

– ETSI TS 119 512 V1.1.1 (protocoale pentru serviciile de păstrare);

– ETSI EN 319 401 V3.1.1; ETSI EN 319 102-1 V1.4.1; ETSI TS 119 172-4 V1.1.1; ETSI TS 119 612 V2.4.1; ETSI TS 119 312;

– ETSI EN 319 122-1, EN 319 132-1, EN 319 142-1 și EN 319 162-1 (formatele CAdES, XAdES, PAdES și ASiC), conform Regulamentului de punere în aplicare (UE) 2026/248;

– IETF RFC 3161 (marca temporală), RFC 4998 (ERS) și RFC 6283 (XMLERS).

Versiunile complete ale standardelor aplicate sunt cele din documentul 00n.

2. Definiții și acronime

2.1. Definiții

– **obiect de păstrare (PO)** — datele transmise spre păstrare: semnătura sau sigiliul, datele semnate ori amprentele acestora;

– **container al obiectului de păstrare (POC)** — obiectul de păstrare împreună cu dovezile de păstrare și metadatele asociate;

– **dovadă de păstrare** — datele (marcă temporală de arhivă, înregistrare de dovezi ERS) care permit demonstrarea existenței și integrității obiectului la un moment dat și a validității semnăturii sau sigiliului;

– **augmentare** — adăugarea de dovezi noi, înainte ca dovezile existente să devină nesigure.

2.2. Acronime

Acronim	Semnificație
ERS	Evidence Record Syntax (RFC 4998 / RFC 6283)
PDS	păstrarea semnăturilor digitale (obiectiv de păstrare, TS 119 511)
PGD	păstrarea datelor generale
AUG	augmentarea dovezilor de păstrare transmise
WST / WTS / WOS	cu stocare / cu stocare temporară / fără stocare
QPS	serviciu calificat de păstrare

3. Descrierea serviciului

3.1. Obiectivele de păstrare

– **PDS** — păstrarea semnăturilor și sigiliilor electronice calificate, prin validare la preluare și dovezi de păstrare reînnoite periodic;

– **PGD** — păstrarea datelor generale (inclusiv nesemnate), prin dovezi ale existenței și integrității lor la un moment dat;

– **AUG** — augmentarea dovezilor de păstrare transmise de abonat.

3.2. Modelele de stocare

Model	Descriere
WST — cu stocare	CERTDIGITAL stochează obiectele și dovezile pe perioada de păstrare
WTS — cu stocare temporară	CERTDIGITAL nu stochează permanent obiectele; dovezile se produc asincron și pot fi preluate de abonat într-o perioadă limitată (secțiunea 3.6); abonatul poate transmite fie obiectele, fie numai amprentele acestora
WOS — fără stocare	CERTDIGITAL nu stochează obiectele; dovezile se produc sincron și se returnează în răspuns; abonatul păstrează datele și dovezile

3.3. Formatele acceptate

– semnături și sigilii: CAdES (EN 319 122-1), XAdES (EN 319 132-1), PAdES (EN 319 142-1), ASiC (EN 319 162-1), conform Regulamentului de punere în aplicare (UE) 2026/248;

– dovezi de păstrare: ERS (RFC 4998), XMLERS (RFC 6283) și augmentare AdES la nivelul B-LTA (EN 319 122-1, 319 132-1, 319 142-1);

– protocol: ETSI TS 119 512, legăturile REST/JSON și SOAP/XML.

Identificatorii formatelor, conform ETSI TS 119 512, anexa A:

Format	Identificator (URI)
CAdES (intrare)	`http://uri.etsi.org/ades/CAdES`
XAdES (intrare)	`http://uri.etsi.org/ades/XAdES`
PAdES (intrare)	`http://uri.etsi.org/ades/PAdES`
ASiC-E (intrare)	`http://uri.etsi.org/ades/ASiC/type/ASiC-E`
Listă de amprente — DigestList (intrare)	`http://uri.etsi.org/19512/format/DigestList`
CAdES Archive Time Stamp V3 (dovadă)	`http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3`
XAdES Archive Time Stamp (dovadă)	`http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp`
PAdES Document Time-Stamp (dovadă)	`http://uri.etsi.org/ades/PAdES/document-time-stamp`
Evidence Record RFC 4998 (dovadă)	`urn:ietf:rfc:4998:EvidenceRecord`
Evidence Record RFC 6283 (dovadă)	`urn:ietf:rfc:6283:EvidenceRecord`
ASiC-ERS (container de ieșire)	`http://uri.etsi.org/ades/ASiC/type/ASiC-ERS`

Funcțiile hash acceptate pentru amprentele transmise: SHA-256, SHA-384, SHA-512.

3.4. Operațiile serviciului (ETSI TS 119 512)

Operație	Rol
RetrieveInfo	metadatele serviciului, profilurile și OID-urile acceptate
PreservePO	transmiterea unui obiect spre păstrare, cu profilul ales
RetrievePO / RetrievePOC	regăsirea obiectului păstrat sau a containerului cu dovezi
UpdatePOC	augmentarea dovezilor
ValidateEvidence	validarea dovezilor, cu raport care indică politica de validare aplicată
DeletePO	ștergerea obiectelor (WST/WTS)
RetrieveTrace	regăsirea jurnalului ciclului de viață al obiectului

Punctul de acces al serviciului: **https://qps.certdigital.ro**, cu autentificarea abonatului prin cheie API, nume de utilizator și parolă, create la înrolarea în sistem.

3.5. Limitări

– se păstrează numai semnăturile și sigiliile valide la momentul preluării; cele nevalide se resping, cu raport de validare;

– dimensiunea maximă a unui obiect de păstrare (WST, WTS, PGD): **500 MB**; pentru WOS, valoarea amprentei: cel mult 512 octeți;

– perioada de păstrare (WST, PGD): **10 ani** de la preluare, conform contractului;

– obiective de performanță: PreservePO — dovezi returnate în cel mult 5 secunde, ValidateEvidence — raport în cel mult 3 secunde, în 95% din cazuri;

– când abonatul transmite numai amprentele obiectelor, păstrarea privește numai amprentele transmise și dovedește existența obiectului numai cât timp funcția hash rămâne sigură; CERTDIGITAL nu răspunde de corespondența dintre amprentele transmise (inclusiv cele folosite la reînnoirea arborelui de amprente) și obiectele originale.

3.6. Profilurile de păstrare

Profilurile sunt descrise conform ETSI TS 119 511 (cl. 6.4) și ETSI TS 119 512 (cl. 5.4.7 și anexa F). Elementele comune tuturor profilurilor:

Element	Valoare
Policy — politica privind dovezile (tip `http://uri.etsi.org/19512/policy/preservation-evidence`)	`urn:oid:1.3.6.1.4.1.47898.10.4` (secțiunea 4.3, împreună cu politica criptografică, secțiunea 4.2)
Policy — politica de validare a semnăturilor (tip `http://uri.etsi.org/19512/policy/signature-validation`), pentru obiectivul PDS când abonatul nu transmite datele de validare	`urn:oid:1.3.6.1.4.1.47898.10.2.1` (secțiunea 4.1)
ProfileValidityPeriod	ValidFrom = data intrării în vigoare a versiunii 2.0 a prezentului document; fără dată de încetare
Specification	https://www.certdigital.ro/repository/politici/certdigital_pspps_ro.pdf (prezentul document; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/)

Element	Valoare
Operații disponibile în toate profilurile	RetrieveInfo

Profilurile nu se modifică în timp; orice schimbare a elementelor de mai jos se face printr-un profil nou, cu identificator nou (TS 119 511, OVR-6.4-13).

Profilul WOS — urn:oid:1.3.6.1.4.1.47898.10.1.1

Element	Valoare
SchemeIdentifier	`http://uri.etsi.org/19512/scheme/pds+wos+aug` (TS 119 512, F.4)
PreservationGoal	PDS (`http://uri.etsi.org/19512/goal/pds`), AUG (`http://uri.etsi.org/19512/goal/aug`)
PreservationStorageModel	WithoutStorage
Operații	PreservePO (obligatorie); ValidateEvidence, RetrieveTrace
Formate de intrare	CAdES, XAdES, PAdES, ASiC-E
EvidenceFormat	CAdES Archive Time Stamp V3; XAdES Archive Time Stamp; PAdES Document Time-Stamp
ExpectedEvidenceDuration	se calculează pentru fiecare dovadă, pe baza politicii criptografice (ETSI TS 119 312), și nu depășește data expirării certificatului TSU care a semnat cea mai recentă marcă temporală de arhivă (07.07.2038 pentru CERTDIGITAL TSA G4), diminuată cu pragurile de la secțiunea 4.2; se returnează în răspuns
Description	păstrarea semnăturilor și sigiliilor prin augmentare la nivelul LTA, fără stocare; abonatul păstrează documentul și îl retransmite înaintea datei recomandate pentru augmentarea următoare

Profilul WST — urn:oid:1.3.6.1.4.1.47898.10.1.2

Element	Valoare
SchemeIdentifier	`http://uri.etsi.org/19512/scheme/pds+wst+aug` (TS 119 512, F.3)
PreservationGoal	PDS, AUG
PreservationStorageModel	WithStorage
Operații	PreservePO, RetrievePO, DeletePO (obligatorii); ValidateEvidence, RetrieveTrace, Search
Formate de intrare	CAdES, XAdES, PAdES, ASiC-E
EvidenceFormat	CAdES Archive Time Stamp V3; XAdES Archive Time Stamp; PAdES Document Time-Stamp
Perioada de păstrare	10 ani de la preluare, conform contractului
Description	păstrarea semnăturilor și sigiliilor cu stocare; augmentarea este declanșată de CERTDIGITAL

Profilul WTS — urn:oid:1.3.6.1.4.1.47898.10.1.3

Element	Valoare
SchemeIdentifier	`http://uri.etsi.org/19512/scheme/pgd+wts+ers` (TS 119 512, F.2)
PreservationGoal	PGD (`http://uri.etsi.org/19512/goal/pgd`), AUG
PreservationStorageModel	WithTemporaryStorage
Operații	PreservePO, RetrievePO (obligatorii); ValidateEvidence, RetrieveTrace

Element	Valoare
Formate de intrare	DigestList (SHA-256, SHA-384, SHA-512) și orice obiect de date, inclusiv CAdES, XAdES, PAdES, ASiC-E
EvidenceFormat	Evidence Record RFC 4998; Evidence Record RFC 6283
PreservationEvidenceRetentionPeriod	30 de zile de la producerea dovezii
ExpectedEvidenceDuration	ca la profilul WOS
Description	dovada existenței datelor, cu înregistrări de dovezi produse asincron și disponibile pentru preluare în perioada de mai sus

Profilul PGD — urn:oid:1.3.6.1.4.1.47898.10.1.4

Element	Valoare
SchemeIdentifier	`http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers` (TS 119 512, F.1)
PreservationGoal	PDS, PGD, AUG
PreservationStorageModel	WithStorage
Operații	PreservePO, RetrievePO, DeletePO (obligatorii); UpdatePOC, ValidateEvidence, RetrieveTrace, Search
Formate de intrare	orice obiect de date, inclusiv CAdES, XAdES, PAdES, ASiC-E
EvidenceFormat	Evidence Record RFC 4998; Evidence Record RFC 6283
Formate de ieșire	ASiC-ERS
Perioada de păstrare	10 ani de la preluare, conform contractului
Description	păstrarea datelor generale și a semnăturilor, cu stocare, prin înregistrări de dovezi reînnoite de CERTDIGITAL

Profilul AUG — urn:oid:1.3.6.1.4.1.47898.10.1.5

Element	Valoare
SchemeIdentifier	— (profil fără schemă definită în TS 119 512)
PreservationGoal	AUG
PreservationStorageModel	WithoutStorage
Operații	PreservePO (cu dovezile existente transmise de abonat); ValidateEvidence, RetrieveTrace
Formate de intrare	Evidence Record RFC 4998 / RFC 6283 împreună cu datele sau amprentele acoperite; semnături CAdES, XAdES, PAdES, ASiC-E cu marcă temporală de arhivă
EvidenceFormat	Evidence Record RFC 4998; Evidence Record RFC 6283; CAdES Archive Time Stamp V3; XAdES Archive Time Stamp; PAdES Document Time-Stamp
ExpectedEvidenceDuration	ca la profilul WOS
Description	augmentarea dovezilor de păstrare emise anterior de CERTDIGITAL sau de alt serviciu de păstrare, după validarea lor

Identificatorii de schemă sunt cei din clauza „Identifier” a fiecărei scheme din TS 119 512 V1.1.1, anexa F. În aceeași anexă, câmpul „SchemeIdentifier” al schemelor F.1, F.3 și F.4 indică alte valori (de exemplu `pgd+wos+aug` în loc de `pds+wos+aug`); CERTDIGITAL folosește identificatorul din clauza „Identifier”.

4. Politicile serviciului

4.1. Politica de validare implicită (OID 1.3.6.1.4.1.47898.10.2.1)

Se aplică tuturor semnăturilor și sigiliilor la preluare, pentru obiectivul PDS. Validarea se face de componenta de validare a serviciului, conform ETSI EN 319 102-1 V1.4.1 și ETSI TS 119 172-4 V1.1.1; ea nu constituie un serviciu calificat de validare în sensul art. 33 și 40 din Regulamentul eIDAS.

– **ancorele de încredere**: Listele de încredere ale statelor membre, accesate prin lista listelor publicată de Comisia Europeană (ETSI TS 119 612 V2.4.1); statutul calificat al semnăturii sau sigiliului se stabilește conform TS 119 172-4;

– **datele de validare**: lanțurile de certificate, CRL-urile și răspunsurile OCSP se colectează de CERTDIGITAL și se includ în dovezi; dacă abonatul transmite el însuși datele de validare, acestea se verifică conform prezentei politici (TS 119 511, OVR-9.3-02);

– **perioada de grație**: validarea finală se face după expirarea unei perioade de grație de 24 de ore de la momentul semnăturii (indicat de marca temporală a semnăturii sau, în lipsa acesteia, de momentul preluării), conform conceptului de perioadă de grație din ETSI EN 319 102-1, astfel încât să fie luate în considerare revocările publicate în termenul legal de 24 de ore;

– **imposibilitatea colectării datelor de validare** (TS 119 511, OVR-6.2-06): CERTDIGITAL reîncearcă colectarea pe durata perioadei de grație; dacă datele nu pot fi obținute nici după aceea, cererea se respinge cu un raport de validare cu rezultatul „nedeterminat” (INDETERMINATE), iar abonatul poate retransmite obiectul împreună cu propriile date de validare;

– semnăturile și sigiliile cu rezultatul „nevalid” (TOTAL-FAILED) se resping, cu raportul de validare.

4.2. Politica criptografică (OID 1.3.6.1.4.1.47898.10.3)

– algoritmi de semnătură acceptați: RSA de cel puțin 3072 de biți; ECDSA cu curbele P-256, P-384, P-521; EdDSA (Ed25519, Ed448), unde formatul permite;

– funcții hash: cel puțin SHA-256;

– algoritmii respectă ETSI TS 119 312 și documentul „Agreed Cryptographic Mechanisms” al ECCG;

– **pragurile de augmentare**: dovezile se augmentează cu cel puțin 3 ani înainte de sfârșitul duratei de viață recomandate a unui algoritm de semnătură și cu cel puțin 5 ani înainte de data la care un algoritm hash este considerat nesigur, precum și înainte de expirarea certificatului TSU care a semnat ultima marcă temporală de arhivă.

Lanțurile ERS se augmentează pe baza pragurilor de mai sus, fără un interval fix.

4.3. Politica privind formatul dovezilor (OID 1.3.6.1.4.1.47898.10.4)

Politica stabilește modul de creare, augmentare și validare a dovezilor (TS 119 511, cl. 6.5):

– **formatul**: formatele de dovadă de la secțiunile 3.3 și 3.6, pentru fiecare profil;

– **crearea**: ERS — arbore de amprente acoperit de o marcă temporală calificată; AdES — adăugarea datelor de validare și a unei mărci temporale de arhivă care acoperă semnătura, datele de validare și datele semnate (nivel LTA); algoritmii sunt cei din politica criptografică (secțiunea 4.2);

– **prestatorii de servicii de încredere utilizați**: numai CERTDIGITAL — serviciul de marcare temporală calificată CERTDIGITAL TSA G4 (politica 0.4.0.2023.1.1) și serviciile de informare privind starea certificatelor ale autorităților emitente ale certificatelor validate; nu se utilizează alți prestatori;

– **validarea dovezilor**: dovezile se validează conform ETSI EN 319 102-1 (pentru AdES) și RFC 4998 / RFC 6283 (pentru ERS), cu ancora de încredere a lanțului certificatului care a semnat marca temporală, respectiv sigiliul serviciului: CERTDIGITAL ROOT CA G4 pentru certificatele G4 și CERTDIGITAL ROOT CA G5 pentru certificatele G5 (inclusiv CERTDIGITAL QPS SERVICE G5), verificabilă prin Lista de încredere a României; operația ValidateEvidence furnizează un raport de validare;

– **augmentarea**: conform secțiunii 5.3;

– **identificarea serviciului și a politicii**: dovezile identifică serviciul prin sigiliul electronic calificat al acestuia (secțiunea 6.3) și prin marca temporală; profilul și politica aplicate se indică în răspunsul la cerere și în jurnalul obiectului.

4.4. Profilul API (OID 1.3.6.1.4.1.47898.10.5)

Interfața respectă ETSI TS 119 512 (secțiunea 3.4); specificația tehnică se pune la dispoziția abonaților.

5. Practicile serviciului

5.1. Preluarea obiectelor

Abonatul transmite obiectul și profilul ales; serviciul verifică formatul și dimensiunea, validează semnătura sau sigiliul (secțiunea 4.1), creează dovezile și confirmă preluarea, cu identificatorul obiectului.

5.2. Generarea dovezilor

Pentru ERS se construiește arborele de amprente și se obține o marcă temporală calificată; pentru AdES se adaugă datele de validare și marca temporală de arhivă (nivel B-LTA). Dovezile se sigilează cu certificatul serviciului.

Pentru obiectivul PDS, păstrarea se realizează în trei etape:

1. **colectarea datelor de validare**, la preluare, dacă nu sunt deja incluse în semnătură sau sigiliu;

2. **atingerea nivelului LTA**, după expirarea perioadei de grație de 24 de ore (secțiunea 4.1) sau la preluare, dacă perioada a expirat deja: se adaugă datele de validare lipsă și o marcă temporală de arhivă care acoperă semnătura, datele de validare și datele semnate; marca temporală de arhivă acoperă direct datele semnate și în cazul semnăturilor detașate;

3. **menținerea nivelului LTA**, la fiecare eveniment de păstrare (secțiunea 5.3): se adaugă o marcă temporală de arhivă nouă, care protejează mărcile temporale anterioare, datele de validare și datele semnate împotriva expirării certificatelor și a slăbirii algoritmilor.

La profilurile cu stocare (WST, PGD), etapa 2 se efectuează automat după expirarea perioadei de grație. La profilurile fără stocare (WOS, AUG), dacă perioada de grație nu a expirat la preluare, răspunsul indică momentul după care abonatul retransmite obiectul pentru finalizarea etapei 2.

5.3. Augmentarea (reînnoirea) dovezilor

CERTDIGITAL monitorizează continuu valabilitatea algoritmilor și a certificatelor folosite în dovezi. La atingerea pragurilor de la secțiunea 4.2 se verifică lanțul existent de dovezi, se adaugă dovezi noi cu algoritmi actuali și mărci temporale noi, iar operația se înregistrează în containerul obiectului (POC) și în jurnale.

Cine declanșează evenimentele de păstrare:

– **profilurile cu stocare (WST, PGD)**: CERTDIGITAL, fără intervenția abonatului;

– **profilurile fără stocare sau cu stocare temporară (WOS, WTS, AUG)**: abonatul. În fiecare răspuns, CERTDIGITAL indică durata estimată de valabilitate a dovezii (expected evidence duration) și data recomandată pentru augmentarea următoare; abonatul păstrează obiectul și dovezile și le retransmite înaintea acestei date. CERTDIGITAL nu răspunde de pierderea capacității de validare dacă abonatul nu retransmite obiectul la timp.

5.4. Protocolul de notificare

Serviciul nu oferă un protocol de notificare în sensul ETSI TS 119 511 (cl. 8.2) și ETSI TS 119 512. Informațiile privind modificarea profilurilor sau a politicilor se publică în depozitul de documente, conform secțiunii 8.7, iar datele recomandate pentru augmentare se comunică în răspunsurile serviciului.

5.5. Regăsirea, validarea și accesul la obiecte

Abonatul sau, cu acordul acestuia, partea care se bazează poate regăsi obiectul sau containerul și poate valida dovezile; raportul indică politica de validare aplicată. Dreptul de acces la obiectele păstrate și la dovezi, precum și dreptul de a solicita jurnalul acțiunilor asupra unui obiect (RetrieveTrace), aparțin abonatului și persoanelor desemnate de acesta în contract (TS 119 511, OVR-6.7-04 și OVR-6.7-05).

5.6. Exportul, ștergerea și sfârșitul perioadei de păstrare

– **WOS și AUG**: obiectele primite se șterg imediat după returnarea răspunsului; nu se stochează obiectele, amprentele sau dovezile, ci numai jurnalele operațiilor (secțiunea 5.7);

– **WTS**: obiectele se șterg după producerea dovezilor; dovezile se păstrează numai pe durata perioadei de preluare din profil (secțiunea 3.6) și se șterg după preluare sau la expirarea acestei perioade (TS 119 511, OVR-9.1-03);

– **WST și PGD**: obiectele se șterg la cererea abonatului (DeletePO) sau la sfârșitul perioadei de păstrare.

Exportul (WST, PGD): la cererea scrisă a abonatului, transmisă la office@certdigital.ro sau prin portalul client, ori la cererea unui alt serviciu de păstrare autorizat de abonat, CERTDIGITAL pune la dispoziție pachetul de export, care conține obiectele păstrate, dovezile și informațiile necesare validării acestora, în format ASiC-ERS (ETSI TS 119 512, anexa A.3.1), necriptat, pus la dispoziție prin portalul client, pe un canal TLS (TS 119 511, OVR-6.1-07, OVR-6.1-08 și OVR-7.16-01).

Sfârșitul perioadei de păstrare (WST, PGD): la expirarea perioadei de păstrare contractate (10 ani) sau la încetarea contractului, obiectele și dovezile se pun la dispoziția abonatului pentru export timp de 30 de zile, după care se șterg, cu excepția cazului în care perioada de păstrare se prelungește prin act adițional (TS 119 511, OVR-6.1-09). La cerere, CERTDIGITAL emite un certificat de ștergere. Ștergerea se face securizat și se jurnalizează.

5.7. Jurnale și trasabilitate

Se înregistrează preluarea, validarea, generarea și augmentarea dovezilor, regăsirea și ștergerea, cu profilul și politicile aplicate. Jurnalele sunt protejate împotriva modificării, se păstrează cel puțin 10 ani de la data înregistrării și se pun la dispoziția evaluatorilor și a ADR.

5.8. Gestionarea incidentelor

Incidentele se tratează și se notifică conform Procedurii de notificare a incidentelor (00q): ADR în cel mult 24 de ore de la luarea la cunoștință (art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS), DNSC (OUG nr. 155/2024; entitate esențială nr. E-210D02), ANSPDCP în 72 de ore, dacă sunt afectate date cu caracter personal, persoanele afectate. Pentru obiectele încredințate, CERTDIGITAL informează abonatul (operatorul datelor) fără întârzieri nejustificate (art. 33 alin. (2) GDPR).

6. Mediul serviciului și controale

6.1. Controale generale

Se aplică Politicile generale CertDigital: gestionarea riscurilor, securitatea informației, personal cu roluri de încredere angajat al CENTRUL DE CALCUL S.A., verificat și instruit, controlul accesului cu autentificare cu cel puțin doi factori, securitatea operațiunilor și a rețelei (segmentare, firewall, comunicații criptate TLS, sisteme de operare securizate), jurnalizare centralizată.

6.2. Securitatea fizică

Infrastructura serviciilor de încredere este găzduită în două centre de date proprii din Târgu Jiu, separate geografic: un centru principal și un centru secundar de rezervă, pregătit să preia serviciile (activ-pasiv), inclusiv cu modul criptografic (HSM). Centrul principal este proiectat după recomandările TIA-942 pentru nivelul Tier 3. Accesul fizic este controlat pe zone de securitate, cu autentificare în patru factori (cheie, cartelă, cod și amprentă, în această ordine).

6.3. Certificatul și cheia serviciului

Element	Valoare
Certificat	CERTDIGITAL Qualified Preservation Service G4 (certificat calificat pentru sigiliu electronic)
Număr de serie	20 11 04 20 94 04 01 06
Emitent	CERTDIGITAL QUALIFIED CA G4
Valabilitate	29.08.2025 – 28.08.2035
Politici	QCP-l-qscd (0.4.0.194112.1.3), 1.3.6.1.4.1.47898.4.2.2.1.2, 1.3.6.1.4.1.47898.10.1
Cheie	RSA 4096, păstrată în modulul Utimaco CryptoServer Se-Series Gen2 (hardware 5.01.4.0), cu firmware-ul CryptoServer CP5 5.1.2.0, în configurația certificată Common Criteria EAL4+ conform EN 419 221-5 (NSCIB-CC-2300142-02) și ca dispozitiv calificat eIDAS (eIDAS-2300143-02, valabil până la 26.05.2030), conform Regulamentului de punere în aplicare (UE) 2025/1946; exponent public mai mic de $2^{16}+1$ (e = 62571), ca la celelalte chei G4; cheia G5 se generează cu e = 65537
Utilizare	sigilarea dovezilor de păstrare și a rapoartelor serviciului

Certificatul conține identificatorul prezentului document (1.3.6.1.4.1.47898.10.1), neschimbat față de versiunea 1.0, și rămâne în uz.

Serviciul se prestează în generația G4 a infrastructurii CERTDIGITAL, cu certificatul de mai sus, și în generația G5, cu certificatul CERTDIGITAL QPS SERVICE G5:

Element	Valoare
Certificat	CERTDIGITAL QPS SERVICE G5 (certificat calificat pentru sigiliu electronic)
Emitent	CERTDIGITAL QCA G5 (DPC CERTDIGITAL G5)
Valabilitate	5 ani de la emitere
Politici	QCP-l-qscd (0.4.0.194112.1.3), 1.3.6.1.4.1.47898.5.2.2.1.2, 1.3.6.1.4.1.47898.10.1
Cheie	RSA 4096 (e = 65537), generată în ceremonia G5 și păstrată în modulul Thales Luna PCIe HSM 7 A790 (dispozitiv calificat eIDAS-2400055-01; Common Criteria NSCIB-CC-2400054-01; FIPS 140-3 nivel 3), în partiția SVG5

Element	Valoare
Utilizare	sigilarea dovezilor de păstrare și a rapoartelor serviciului (keyUsage digitalSignature, nonRepudiation)

Copia de rezervă a cheii G4 este criptată cu cheia master a HSM (MBK) și poate fi restaurată numai într-un HSM certificat, sub control dual; copia de rezervă a cheii G5 se realizează prin clonarea criptată a partiției SVG5 în al doilea modul Thales Luna, sub control multipersoană (M din N), cu proces-verbal (DPC CERTDIGITAL G5, secțiunea 6.2.4).

6.4. Marcarea temporală

Mărcile temporale utilizate în dovezi sunt mărci temporale electronice calificate emise de CERTDIGITAL TSA G4. CERTDIGITAL nu utilizează o TSA de rezervă; dacă TSA nu este disponibilă, cererile de păstrare și de augmentare se pun în coadă și se finalizează după restabilire, fără emiterea de dovezi incomplete, iar abonatul este informat.

6.5. Sincronizarea timpului

Toate sistemele serviciului sunt sincronizate cu sursa de timp UTC a CERTDIGITAL (documentul „Sursa de timp”, 00u).

6.6. Disponibilitate și continuitate

Serviciul este disponibil 24/7, cu o disponibilitate-țintă de 99,5% pe an; întreruperile planificate se anunță pe site cu cel puțin 24 de ore înainte. Datele serviciului se replică în centrul de date secundar la cel mult 5 minute; durata maximă de restabilire este de 24 de ore (PO/SI/63). Comutarea se testează anual.

7. Obligații

7.1. Obligațiile CERTDIGITAL

Operarea serviciului conform prezentului document; protecția cheii serviciului; validarea la preluare; crearea și augmentarea dovezilor la timp; păstrarea obiectelor (WST) pe perioada contractată; publicarea documentației; notificarea incidentelor.

7.2. Obligațiile abonatului

Transmiterea obiectelor în formatele acceptate; alegerea profilului potrivit; pentru WOS, WTS și AUG, păstrarea propriilor date și dovezi și retransmiterea lor înaintea datei recomandate pentru augmentarea următoare (secțiunea 5.3); protecția datelor de acces; respectarea contractului.

7.3. Obligațiile părții care se bazează

Validarea dovezilor cu instrumente conforme ETSI EN 319 102-1 sau prin ValidateEvidence; verificarea statutului calificat al serviciului în Lista de încredere a României; respectarea limitărilor din prezentul document.

8. Răspundere și aspecte juridice

8.1. Răspunderea

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

CERTDIGITAL nu răspunde pentru prejudiciile rezultate din: utilizarea serviciului peste limitările notificate în prealabil; semnăturile sau sigiliile nevalide la preluare, respinse conform politicii de validare; pierderea datelor sau a dovezilor păstrate de abonat (WOS, WTS după preluare, AUG) ori neretransmiterea lor înaintea datei recomandate pentru augmentare; nerespectarea de către abonat a obligațiilor sale; 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.

8.2. Asigurarea

CENTRUL DE CALCUL S.A. deține, pentru fiecare dintre cele două servicii de păstrare calificată (a semnăturilor electronice calificate și a sigiliilor electronice calificate), câte 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 fiecare poliță, ADR, în calitate de organism de supraveghere, are calitatea de asigurat adițional. Polițele se reînnoiesc înainte de expirare; datele lor de identificare (asigurătorul, seria și numărul, perioada de valabilitate) sunt comunicate ADR și se pun la dispoziție la cerere.

8.3. Protecția datelor cu caracter personal

Pentru datele de identificare și de cont ale abonatului, CERTDIGITAL este operator. Pentru datele cuprinse în obiectele încredințate spre păstrare, CERTDIGITAL acționează ca persoană împuternicită a abonatului, numai pe baza instrucțiunilor documentate ale acestuia, în condițiile art. 28 GDPR și ale contractului serviciului. Detaliile sunt în Politica de protecție a datelor (00d); responsabilul cu protecția datelor: dpo@centruldecalcul.ro.

8.4. Tarife

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

8.5. 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).

8.6. 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: Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 (art. 34 și 40); Regulamentele de punere în aplicare (UE) 2025/2530, 2025/1946 și 2026/248; Directiva (UE) 2022/2555 și Regulamentul de punere în aplicare (UE) 2024/2690; Regulamentul (UE) 2016/679; Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026 și deciziile ADR; OUG nr. 155/2024; Legea nr. 190/2018; Codul civil, Legea nr. 193/2000, OUG nr. 34/2014 și OG nr. 38/2015. Standardele aplicate sunt cele din documentul 00n. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

8.7. 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 serviciilor calificate se comunică ADR cu cel puțin o lună înainte de aplicare (cu cel puțin trei luni în cazul încetării unui serviciu). Abonații și părțile care se bazează sunt informați prin publicare pe site cu cel puțin 30 de zile înainte de intrarea în vigoare. Corecturile de redactare care nu modifică drepturile sau obligațiile părților se publică cu versiune nouă, fără termen de preaviz.

8.8. Încetarea serviciului

Încetarea serviciului se face conform Planului de încetare a serviciilor (00r) și anexei acestuia pentru păstrare. ADR este informată cu cel puțin 3 luni înainte (art. 24 alin. (2) lit. (a) din Regulamentul eIDAS), iar în cazul unei încetări neprevăzute, în cel mult 24 de ore. Abonații sunt informați și pot exporta obiectele și dovezile; obiectele păstrate se transferă, după caz, către un alt prestator calificat; înregistrările se păstrează 10 ani prin custode.

9. Evaluarea conformității

Serviciul este evaluat de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162, cel puțin o dată la 24 de luni, inclusiv în privința cerințelor de la art. 21 din Directiva (UE) 2022/2555 (art. 20 din Regulamentul eIDAS). ADR este informată cu cel puțin o lună înainte de evaluarea planificată și poate participa ca observator; raportul se transmite ADR în cel mult 3 zile lucrătoare de la primire. CERTDIGITAL efectuează anual un audit intern, realizat de personal independent de operarea serviciului.