Politica și declarația de practici a serviciului calificat de marcare temporală

CertDigital Timestamping Authority

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:**
1.7	—	Politica serviciilor de marcare temporală (versiunea anterioară)	06/10/2025
1.4	—	Declarația practicilor de marcare temporală, DPPC-TSA (versiunea anterioară)	05/10/2025
2.0	Ofițer de Securitate IT	Document unic: politica (Partea I) și declarația de practici (Partea a II-a) a serviciului calificat de marcare temporală, conform ETSI EN 319 421 / EN 319 422 și Reg. (UE) 2025/1929; înlocuiește PMT v1.7 și DPPC-TSA v1.4; temeiul publicării tarifelor: art. 11 alin. (1) din Legea nr. 214/2024	22/10/2026
2.1	Ofițer de Securitate IT	Legătura ANPC pentru SAL devine https://anpc.ro/sal; trimiterile la documentele asociate, la versiunile în vigoare (PG v2.1, TC-TSA v2.1, DPC CERTDIGITAL G4 v2.1, DPC CERTDIGITAL G5 v1.1); tabelul de identificare arată versiunea și data în vigoare	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
2.3	Ofițer de Securitate IT	Securitatea fizică și a mediului (11.8): accesul se descrie ca autentificare în mai mulți factori, fără enumerarea factorilor, care rămân în documentația internă de securitate; conținutul neschimbat în rest	03/11/2026

Cuprins

PARTEA I – Politica serviciului 7
1. Introducere 7
1.1. Prezentare generală 7
1.2. Identificarea documentului 7
1.3. Participanții 8
1.4. Utilizarea mărcilor temporale 8
1.5. Relația cu alte documente 8
1.6. Administrarea documentului 9
2. Referințe normative 10
3. Definiții și acronime 11
3.1. Definiții 11
3.2. Acronime 11
4. Cerințele politicii 12
4.1. Serviciul 12
4.2. Precizia timpului 12
4.3. Cheia TSU 12
4.4. Disponibilitatea 13
4.5. Registrul mărcilor temporale 13
5. Obligații și răspundere 14
5.1. Obligațiile TSA 14
5.2. Obligațiile abonatului 14
5.3. Obligațiile părții care se bazează 14
5.4. Incidente și compromiterea cheii 14
5.5. Răspunderea 14
5.6. Asigurarea 15
6. Practicile TSA (rezumat) 16
6.1. Controale 16
6.2. Evaluarea conformității 16
6.3. Încetarea serviciului 16
7. Aspecte comerciale și juridice 17

7.1. Tarife 17
7.2. Protecția datelor cu caracter personal 17
7.3. Modificări 17
7.4. Soluționarea litigiilor 17
7.5. Legea aplicabilă și cadrul legal 17
7.6. Alte prevederi 18
PARTEA A II-A – Declarația de practici 19
8. Concepte generale 19
8.1. Serviciul de marcare temporală 19
8.2. Participanții 19
8.3. Politica și declarația de practici 19
9. Politica de marcare temporală 20
9.1. Generalități 20
9.2. Identificarea 20
9.3. Comunitatea utilizatorilor și aplicabilitatea 20
10. Politici și practici 21
10.1. Evaluarea riscurilor 21
10.2. Declarația practicilor 21
10.2.1. Formatul mărcii temporale 21
10.2.2. Precizia timpului 21
10.2.3. Limitările serviciului 21
10.2.4. Obligațiile abonaților 21
10.2.5. Obligațiile părților care se bazează 21
10.2.6. Verificarea mărcii temporale 21
10.2.7. Legea aplicabilă 22
10.2.8. Disponibilitatea serviciului 22
10.3. Termeni și condiții 22
10.3.1. Publicarea 22
10.3.2. Durata de păstrare a jurnalelor 22
10.4. Politica de securitate a informației 22
10.5. Obligațiile TSA 22
10.6. Informații pentru părțile care se bazează 22
11. Managementul și operarea TSA 23

11.1. Introducere 23
11.2. Organizarea internă 23
11.3. Personalul 23
11.4. Gestionarea activelor 23
11.5. Controlul accesului 23
11.6. Controale criptografice 23
11.6.1. Generarea cheii TSU 23
11.6.2. Protecția cheii private a TSU 23
11.6.3. Certificatul TSU 24
11.6.4. Reînnoirea cheii TSU 24
11.6.5. Ciclul de viață al hardware-ului criptografic 25
11.6.6. Sfârșitul ciclului de viață al cheii TSU 25
11.7. Marcarea temporală 25
11.7.1. Emiterea mărcii 25
11.7.2. Sincronizarea ceasului cu UTC 25
11.8. Securitatea fizică și a mediului 25
11.9. Securitatea operațiunilor 25
11.10. Securitatea rețelei 25
11.11. Gestionarea incidentelor 26
11.12. Colectarea dovezilor 26
11.13. Continuitatea activității 26
11.14. Încetarea TSA 26
11.15. Conformitatea 26

PARTEA I – Politica serviciului

1. Introducere

1.1. Prezentare generală

Prezentul document este Politica și declarația de practici a serviciului calificat de marcare temporală CertDigital (PDP-QTST). Partea I, politica serviciului, stabilește regulile aplicate de CENTRUL DE CALCUL S.A. (marca CertDigital, denumită în continuare „CERTDIGITAL"), prestator de servicii de încredere calificat, pentru emiterea mărcilor temporale electronice calificate, în sensul art. 3 pct. 34 și al art. 42 din Regulamentul (UE) nr. 910/2014. O marcă temporală electronică calificată beneficiază de prezumția exactității datei și orei pe care le indică și a integrității datelor cu care sunt legate data și ora (art. 41 alin. (2)).

Politica respectă ETSI EN 319 421 V1.3.1 și ETSI EN 319 422 V1.1.1, cu adaptările din Regulamentul de punere în aplicare (UE) 2025/1929, precum și ETSI EN 319 401 V3.1.1 și Regulamentul de punere în aplicare (UE) 2025/2530. Practicile prin care sunt îndeplinite cerințele de mai jos sunt descrise în Partea a II-a, declarația de practici a autorității de marcare temporală, a cărei structură urmează ETSI EN 319 421.

1.2. Identificarea documentului

Element	Valoare
Titlu	Politica și declarația de practici a serviciului calificat de marcare temporală CertDigital
Titlu în limba engleză	CertDigital Qualified Time-Stamping Service Policy and Practice Statement
Cod	PDP-QTST
Versiune	2.3
Data	03.11.2026
Politica aplicată mărcilor temporale	ETSI BTSP — Best practices Time-Stamp Policy, OID **0.4.0.2023.1.1** (ETSI EN 319 421)
Declarația de marcă temporală calificată	esi4-qtstStatement-1, OID 0.4.0.19422.1.1 (ETSI EN 319 422), inclusă în fiecare marcă
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-qtst_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Documentul se identifică prin cod și versiune și nu are un OID propriu: serviciul de marcare temporală nu are un arc propriu în CERTDIGITAL_OID_MAP, iar mărcile temporale se identifică prin politica BTSP (secțiunea 9.2).

Versiunea 2.0 reunește politica și declarația de practici ale serviciului într-un singur document și înlocuiește:

– documentele aprobate Politica serviciilor de marcare temporală CertDigital (PMT), versiunea 1.7, și Declarația practicilor de certificare CertDigital Timestamping Authority (DPPC-TSA), versiunea 1.4;

– proiectele neaprobate ale versiunii 2.0, PMT v2.0 și D-TSA v2.0 (Declarația practicilor de marcare temporală, DPC-TSA), unite în prezentul document;

– „Declarația politicilor și practicilor de marcare temporală", versiunea 1.4, care se retrage.

1.3. Participanții

– **autoritatea de marcare temporală (TSA)**: CERTDIGITAL, care răspunde de serviciu în ansamblu;

– **unitatea de marcare temporală (TSU)**: sistemul care emite mărcile, identificat prin certificatul CERTDIGITAL TSA G4 și, după înlocuirea acestuia, prin certificatul CERTDIGITAL TSA G5 (secțiunile 4.3 și 11.6);

– **abonatul**: persoana fizică sau juridică ce a încheiat contract cu CERTDIGITAL pentru utilizarea serviciului;

– **partea care se bazează**: orice persoană care se bazează pe o marcă temporală emisă de CERTDIGITAL.

Autoritatea pentru Digitalizarea României (ADR) este organismul de supraveghere al serviciului (secțiunea 7.5), iar conformitatea serviciului este evaluată de un organism de evaluare a conformității acreditat (secțiunea 6.2).

1.4. Utilizarea mărcilor temporale

Mărcile temporale se utilizează pentru a dovedi existența unor date electronice la un anumit moment, inclusiv în semnăturile și sigiliile electronice avansate și calificate (formatele de nivel T, LT și LTA) și în dovezile serviciilor de păstrare și arhivare. Serviciul nu certifică conținutul datelor marcate.

1.5. Relația cu alte documente

Se aplică, în completarea prezentului document, următoarele documente ale CERTDIGITAL:

– Politici generale CertDigital (PG);

– Sursa de timp precisă, legată de ora universală (00u);

– Procedura de notificare a incidentelor (00q); Planul de încetare a serviciilor (00r);

– Procedura de continuitate operațională și de recuperare în caz de dezastru (PO/SI/63);

– Politica de protecție a datelor cu caracter personal (00d);

– Lista standardelor (00n);

– DPC CERTDIGITAL G4, pentru certificatul CERTDIGITAL TSA G4, și DPC CERTDIGITAL G5, pentru certificatul CERTDIGITAL TSA G5;
– Termenii și condițiile serviciului de marcare temporală calificată (TC-TSA) și Contractul-cadru de furnizare a serviciului de marcare temporală calificată (CTR-TSA).

1.6. 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.

2. Referințe normative

Serviciul este furnizat în conformitate cu următoarele acte normative și standarde:

– Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 (denumit în continuare „Regulamentul eIDAS”), în special art. 24, 41 și 42;

– Regulamentul de punere în aplicare (UE) 2025/1929 (mărcile temporale electronice calificate) și 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);

– Directiva (UE) 2022/2555 și Regulamentul de punere în aplicare (UE) 2024/2690;

– Regulamentul (UE) 2016/679 și Legea nr. 190/2018;

– Legea nr. 214/2024 (în special art. 8), Ordinul MEDAT nr. 102/2026 și deciziile ADR;

– OUG nr. 155/2024;

– Codul civil, Legea nr. 193/2000, OUG nr. 34/2014 și OG nr. 38/2015;

– ETSI EN 319 401 V3.1.1; ETSI EN 319 421 V1.3.1; ETSI EN 319 422 V1.1.1;

– IETF RFC 3161, actualizat prin RFC 5816; IETF RFC 9110 (HTTP).

Lista completă a standardelor aplicate este în documentul 00n.

3. Definiții și acronime

3.1. Definiții

– **marcă temporală (TST)** — date în format electronic care leagă alte date în format electronic de un anumit moment, dovedind că acestea existau la acel moment (art. 3 pct. 33 din Regulamentul eIDAS);

– **autoritatea de marcare temporală (TSA)** — CERTDIGITAL, care răspunde de serviciu;

– **unitatea de marcare temporală (TSU)** — ansamblul hardware și software, cu o singură cheie de semnare activă, care emite mărcile;

– **UTC** — timpul universal coordonat.

3.2. Acronime

Acronim	Semnificație
ADR	Autoritatea pentru Digitalizarea României
ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
BTSP	Best practices Time-Stamp Policy (ETSI EN 319 421)
CRL	lista certificatelor revocate (Certificate Revocation List)
DNSC	Directoratul Național de Securitate Cibernetică
GNSS	sistem global de navigație prin satelit (Global Navigation Satellite System)
HSM	modul criptografic hardware
MBK	cheia master a HSM (Master Backup Key), cu care se criptează copia de rezervă a cheii TSU
NIST	National Institute of Standards and Technology (SUA)
NTP	Network Time Protocol
OCSP	protocolul de verificare online a stării certificatelor (Online Certificate Status Protocol)
PDS	declarația de informare a PKI (PKI Disclosure Statement) a autorității care a emis certificatul TSU, la care trimite declarația QcPDS din certificat
QTST	marcă temporală electronică calificată
TSA / TSU	autoritate / unitate de marcare temporală
TST	marcă temporală (time-stamp token)

4. Cerințele politicii

4.1. Serviciul

– cererile și răspunsurile respectă protocolul IETF RFC 3161, actualizat prin RFC 5816, și profilul ETSI EN 319 422; transportul se face prin HTTPS (RFC 9110), conform Regulamentului de punere în aplicare (UE) 2025/1929;

– cererea conține numai amprenta (valoarea hash) a datelor; datele nu se transmit către CERTDIGITAL;

– algoritmii hash acceptați în cereri: SHA-256, SHA-384, SHA-512;

– marca temporală este semnată cu cheia TSU: cu sha256WithRSAEncryption pentru CERTDIGITAL TSA G4 și cu sha512WithRSAEncryption pentru CERTDIGITAL TSA G5;

– marca conține: identificatorul politicii (0.4.0.2023.1.1), amprenta primită, un număr de serie unic, data și ora UTC, precizia (accuracy = 1 s), declarația esi4-qtstStatement-1 și, la cerere, nonce-ul și certificatul TSU.

Punctul de acces al serviciului: **https://ca.certdigital.ro/tsag3/**. Autentificarea se face cu adresa de e-mail și parola contului de abonat: adresa de e-mail este exact cea folosită la generarea certificatului emis de CERTDIGITAL, iar parola se comunică separat, pe un canal securizat.

4.2. Precizia timpului

Data și ora din marca temporală sunt sincronizate cu timpul universal coordonat (UTC) cu o precizie de ±1 secundă. Sursa de timp este descrisă în documentul „Sursa de timp” (00u): două servere de timp GNSS, câte unul în fiecare centru de date, și o sursă independentă de GNSS. Dacă sincronizarea nu poate fi garantată în limita de precizie, TSU încetează emiterea mărcilor până la restabilirea sincronizării, iar evenimentul se înregistrează.

4.3. Cheia TSU

Element	Valoare
Certificat	CERTDIGITAL TSA G4, emis de CERTDIGITAL QUALIFIED CA G4 (certificat calificat pentru sigiliu electronic, QCP-l-qscd)
Valabilitate certificat	18.07.2023 – 07.07.2038
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)
Utilizarea cheii	numai pentru semnarea mărcilor temporale (extKeyUsage timeStamping, critic); cel mult până la înlocuirea cu certificatul CERTDIGITAL TSA G5 și, în orice caz, nu după 07.07.2035
Copie de rezervă	criptată cu cheia master a HSM (MBK), restaurabilă numai într-un HSM certificat, sub control dual (M din N)

Pentru CERTDIGITAL TSA G5:

Element	Valoare
Certificat	CERTDIGITAL TSA G5, emis de CERTDIGITAL QCA G5 (certificat calificat pentru sigiliu electronic, QCP-l-qscd)
Valabilitate certificat	3 ani de la emitere
Cheie	RSA 3072 (e = 65537), generată 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 certificatelor de serviciu G5 (SVG5)
Utilizarea cheii	numai pentru semnarea mărcilor temporale (extKeyUsage timeStamping, critic), cu sha512WithRSAEncryption; cel mult 2 ani de la emiterea certificatului (ETSI EN 319 421, TIS-7.6.7-04)
Copie de rezervă	prin clonarea criptată a partiției în al doilea modul Thales Luna, sub control multipersoană (M din N), cu proces-verbal (DPC CERTDIGITAL G5, secțiunea 6.2.4)

Cheia privată a TSU nu se utilizează în afara HSM-ului și nu se utilizează după expirarea perioadei de utilizare. La compromiterea cheii se aplică secțiunea 5.4.

4.4. Disponibilitatea

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. CERTDIGITAL nu operează o unitate de marcare temporală de rezervă; la indisponibilitate se aplică Procedura de continuitate operațională și de recuperare în caz de dezastru (PO/SI/63), cu o durată maximă de restabilire de 8 ore.

4.5. Registrul mărcilor temporale

CERTDIGITAL ține registrul electronic operativ al mărcilor temporale emise (art. 8 alin. (2) din Legea nr. 214/2024), consultabil la https://ca.certdigital.ro/tsa/. Înregistrările privind mărcile emise și funcționarea TSU se păstrează cel puțin 10 ani de la data înregistrării.

5. Obligații și răspundere

5.1. Obligațiile TSA

CERTDIGITAL:

– emite mărcile temporale conform politicii (Partea I) și declarației de practici (Partea a II-a);

– protejează cheia TSU și menține sincronizarea cu UTC;

– publică certificatul TSU, prezentul document și termenii și condițiile;

– păstrează înregistrările conform secțiunii 4.5;

– informează abonații și ADR conform secțiunii 5.4 la incidentele care afectează serviciul.

5.2. Obligațiile abonatului

Abonatul:

– utilizează serviciul conform contractului și termenilor și condițiilor;

– verifică semnătura mărcii temporale primite și corespondența amprentei cu datele sale;

– protejează datele de acces la serviciu și informează CERTDIGITAL despre orice utilizare neautorizată.

5.3. Obligațiile părții care se bazează

Partea care se bazează:

– verifică semnătura mărcii temporale și corespondența amprentei cu datele;

– verifică validitatea certificatului TSU la momentul emiterii mărcii (OCSP sau CRL) și statutul calificat al serviciului în Lista de încredere a României;

– ține cont de algoritmii utilizați și de evoluția rezistenței acestora în timp.

5.4. Incidente și compromiterea cheii

CERTDIGITAL notifică incidentele 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, și persoanele afectate. La compromiterea sau suspiciunea de compromitere a cheii TSU ori la pierderea sincronizării care afectează mărcile emise, CERTDIGITAL oprește emiterea, revocă certificatul TSU, informează abonații și părțile care se bazează și publică pe site informațiile necesare identificării mărcilor afectate.

5.5. Răspunderea

CERTDIGITAL răspunde, conform art. 13 din Regulamentul eIDAS, pentru prejudiciile cauzate cu intenție sau din neglijență oricărei persoane fizice sau juridice, inclusiv titularilor 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 și recognoscibile de terți; nerespectarea de către abonat a obligațiilor sale; neverificarea de către partea care se bazează a semnăturii mărcii și a stării certificatului TSU; 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.

5.6. Asigurarea

CENTRUL DE CALCUL S.A. deține, pentru serviciul de marcare temporală calificată, 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.

6. Practicile TSA (rezumat)

6.1. Controale

CERTDIGITAL aplică pentru serviciul de marcare temporală politicile generale ale prestatorului (Politici generale CertDigital): gestionarea riscurilor, securitatea informației, personal cu roluri de încredere, control dual pentru operațiile cu cheia TSU, securitate fizică în două centre de date, securitatea operațiunilor și a rețelei (sunt permise numai fluxurile necesare: HTTPS pentru RFC 3161, NTP către sursele de timp, administrare din rețeaua internă dedicată), jurnalizare centralizată și evaluarea anuală a riscurilor. Detaliile sunt descrise în Partea a II-a (capitolele 10 și 11).

6.2. Evaluarea conformității

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

6.3. Încetarea serviciului

Încetarea serviciului se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530, și anexei acestuia pentru marcarea temporală. 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. Cheia TSU se distruge pe bază de proces-verbal; certificatul TSU se revocă; înregistrările se păstrează 10 ani prin custode.

7. Aspecte comerciale și juridice

7.1. 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). Verificarea mărcilor temporale și informațiile privind starea certificatului TSU sunt gratuite.

7.2. Protecția datelor cu caracter personal

Serviciul prelucrează numai amprenta datelor; documentul marcat nu este transmis către CERTDIGITAL. Datele de cont ale abonatului și jurnalele tehnice se prelucrează conform Regulamentului (UE) 2016/679, Legii nr. 190/2018 și Politicii de protecție a datelor cu caracter personal (00d). Responsabilul cu protecția datelor: dpo@centruldecalcul.ro.

7.3. 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 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.

7.4. Soluționarea litigiilor

Litigiile se soluționează pe cale amiabilă, pe baza unei reclamații transmise la office@certdigital.ro, la care CERTDIGITAL răspunde în cel mult 30 de zile. În lipsa unei soluții amiabile, litigiile cu profesioniștii sunt de competența instanțelor de la sediul CENTRUL DE CALCUL S.A. (Târgu Jiu). Consumatorii se pot adresa instanțelor competente potrivit legii, inclusiv celor de la domiciliul lor, și pot apela la procedurile de soluționare alternativă a litigiilor (SAL) prevăzute de OG nr. 38/2015 (ANPC – https://anpc.ro/sal).

7.5. 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 enumerate în capitolul 2. Standardele aplicate sunt cele din documentul 00n. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

7.6. Alte prevederi

CERTDIGITAL urmărește accesibilitatea serviciilor pentru persoanele cu dizabilități (art. 15 din Regulamentul eIDAS). Prezentul document este redactat în limba română; în caz de neconcordanță cu o traducere, prevalează versiunea în limba română.

PARTEA A II-A – Declarația de practici

8. Concepte generale

Partea a II-a este declarația de practici a autorității de marcare temporală CERTDIGITAL TSA. Ea descrie practicile prin care CERTDIGITAL îndeplinește cerințele politicii din Partea I și ale ETSI EN 319 421 V1.3.1 și ETSI EN 319 422 V1.1.1, cu adaptările din Regulamentul de punere în aplicare (UE) 2025/1929, la emiterea mărcilor temporale electronice calificate (art. 42 din Regulamentul eIDAS). Structura Părții a II-a urmează ETSI EN 319 421. Identificarea documentului, participanții, referințele normative și definițiile sunt cele din Partea I (capitolele 1–3).

8.1. Serviciul de marcare temporală

Serviciul cuprinde emiterea mărcilor temporale (TSU) și gestionarea serviciului (monitorizare, sincronizarea timpului, gestionarea cheii). Abonatul transmite o cerere RFC 3161 care conține amprenta datelor; TSU adaugă data și ora UTC, semnează cu cheia TSU și returnează marca.

8.2. Participanții

Participanții (TSA, TSU, abonatul și partea care se bazează) sunt cei din secțiunea 1.3; datele de identificare și de contact ale TSA sunt în secțiunea 1.6.

8.3. Politica și declarația de practici

Politica serviciului (Partea I) stabilește cerințele; prezenta declarație de practici (Partea a II-a) descrie modul în care sunt îndeplinite. Documentul se publică la https://www.certdigital.ro/repository/.

9. Politica de marcare temporală

9.1. Generalități

Mărcile temporale calificate CERTDIGITAL sunt emise conform politicii ETSI BTSP (OID 0.4.0.2023.1.1, EN 319 421), cu precizie de ±1 s față de UTC, și conțin declarația QTST esi4-qtstStatement-1 (EN 319 422).

9.2. Identificarea

Identificatorul politicii din câmpul policy al mărcii: **0.4.0.2023.1.1**. Nu se utilizează alți identificatori de politică pentru mărcile temporale; identificatorii 1.3.6.1.4.1.47898.4.2.2.1.2 (politica certificatului CERTDIGITAL TSA G4) și 1.3.6.1.4.1.47898.5.2.2.1.2 (politica certificatului CERTDIGITAL TSA G5) nu sunt politici de marcare temporală.

9.3. Comunitatea utilizatorilor și aplicabilitatea

Serviciul este disponibil abonaților CERTDIGITAL, iar mărcile pot fi utilizate de orice parte care se bazează. Mărcile sunt potrivite pentru semnături și sigilii electronice de nivel T, LT și LTA (ETSI EN 319 122, 319 132, 319 142), pentru dovezile serviciilor de păstrare și arhivare și pentru orice dovadă a existenței datelor la un moment dat.

10. Politici și practici

10.1. Evaluarea riscurilor

Riscurile serviciului se evaluează cel puțin anual și la fiecare modificare semnificativă, conform Politicilor generale CertDigital (cap. 3). Riscurile principale tratate: compromiterea cheii TSU, pierderea sincronizării cu UTC, indisponibilitatea serviciului, vulnerabilitățile sistemului de operare al TSU.

10.2. Declarația practicilor

10.2.1. Formatul mărcii temporale

Mărcile respectă RFC 3161, RFC 5816 și ETSI EN 319 422 (secțiunea 7). Sunt acceptate cereri cu amprente SHA-256, SHA-384 și SHA-512; marca emisă de CERTDIGITAL TSA G4 este semnată cu sha256WithRSAEncryption și cheia RSA 4096 a TSU, iar cea emisă de CERTDIGITAL TSA G5, cu sha512WithRSAEncryption și cheia RSA 3072 a TSU.

10.2.2. Precizia timpului

±1 secundă față de UTC, declarată în câmpul accuracy al fiecărei mărci.

10.2.3. Limitările serviciului

Serviciul nu verifică datele marcate și nu păstrează amprentele după emiterea mărcii, cu excepția jurnalelor de la secțiunea 11.12. Valabilitatea unei mărci poate fi extinsă prin marcare temporală ulterioară (arhivare), înainte ca algoritmii utilizați să devină nesiguri.

10.2.4. Obligațiile abonaților

Abonatul utilizează serviciul conform contractului, verifică semnătura mărcii primite și corespondența amprentei și protejează datele de acces.

10.2.5. Obligațiile părților care se bazează

Partea care se bazează verifică semnătura mărcii, corespondența amprentei cu datele, validitatea certificatului TSU la momentul emiterii (OCSP sau CRL) și statutul calificat al serviciului în Lista de încredere a României.

10.2.6. Verificarea mărcii temporale

Marca se verifică cu certificatul TSU care a semnat-o și cu lanțul acestuia, publicate la https://certs.certdigital.ro/: CERTDIGITAL TSA G4 → CERTDIGITAL QUALIFIED CA G4 → CERTDIGITAL ROOT CA G4, respectiv CERTDIGITAL TSA G5 → CERTDIGITAL QCA G5 → CERTDIGITAL ROOT CA G5. Starea certificatului TSU se verifică prin http://ocsp.g4.certdigital.ro sau http://crl.certdigital.ro/certdigital_qualified_g4.crl (TSA G4),

respectiv prin http://ocsp.g5.certdigital.ro sau http://crl.certdigital.ro/certdigital_qualified_g5.crl (TSA G5).

10.2.7. Legea aplicabilă

Dreptul român, sub rezerva dispozițiilor direct aplicabile ale dreptului Uniunii Europene (secțiunea 7.5).

10.2.8. Disponibilitatea serviciului

24/7, cu disponibilitate-țintă de 99,5% pe an; întreruperile planificate se anunță pe site cu cel puțin 24 de ore înainte. Punctul de acces: **https://ca.certdigital.ro/tsag3/** (RFC 3161, prin HTTPS). Autentificarea se face conform secțiunii 4.1.

10.3. Termeni și condiții

10.3.1. Publicarea

Termenii și condițiile serviciului (TC-TSA), care cuprind declarația de informare a TSA (TSA disclosure statement, ETSI EN 319 421, anexa B), se publică în depozit și se pun la dispoziția abonatului înainte de contractare.

10.3.2. Durata de păstrare a jurnalelor

Jurnalele de funcționare ale TSU și înregistrările privind mărcile emise se păstrează cel puțin 10 ani de la data înregistrării.

10.4. Politica de securitate a informației

Se aplică Politicile generale CertDigital (PG), aprobate de Directorul General și comunicate personalului.

10.5. Obligațiile TSA

CERTDIGITAL respectă cerințele politicii (Partea I) și ale prezentei declarații, inclusiv prin furnizori, și răspunde față de abonați și părțile care se bazează conform art. 13 din Regulamentul eIDAS (secțiunea 5.5). Asigurarea serviciului este descrisă în secțiunea 5.6.

10.6. Informații pentru părțile care se bazează

CERTDIGITAL publică certificatele TSU (CERTDIGITAL TSA G4 și CERTDIGITAL TSA G5), lanțurile de certificare, prezentul document și informațiile privind statutul calificat. Registrul electronic operativ al mărcilor temporale (art. 8 alin. (2) din Legea nr. 214/2024) este consultabil la https://ca.certdigital.ro/tsa/.

11. Managementul și operarea TSA

11.1. Introducere

Controalele de mai jos se aplică în completarea Politicilor generale CertDigital.

11.2. Organizarea internă

Serviciul este coordonat de directorul tehnic; ofițerul de securitate IT verifică aplicarea controalelor. Directorul General aprobă prezentul document (politica și declarația de practici) și modificările semnificative.

11.3. Personalul

Personalul cu roluri de încredere (administratori de sistem, operatori, custozi HSM, auditori de sistem) este angajat al CENTRUL DE CALCUL S.A., verificat, instruit și numit prin decizie, cu separarea sarcinilor (PG, cap. 5).

11.4. Gestionarea activelor

Componentele TSU (servere, HSM, servere de timp) sunt inventariate, cu proprietar și clasificare „Restricționat”.

11.5. Controlul accesului

Accesul administrativ la TSU se face cu conturi nominale și autentificare cu cel puțin doi factori, din rețeaua internă dedicată; activitățile sunt jurnalizate.

11.6. Controale criptografice

11.6.1. Generarea cheii TSU

Cheia TSU a fost generată într-un modul criptografic hardware, sub control dual, iar certificatul CERTDIGITAL TSA G4 a fost emis la 18.07.2023 de CERTDIGITAL QUALIFIED CA G4. Cheia se află în modulul Utimaco CryptoServer Se-Series Gen2, firmware CryptoServer CP5 5.1.2.0 (CC EAL4+ EN 419 221-5; eIDAS-2300143-02). Cheia are exponent public mai mic de $2^{16}+1$ (e = 60551). Cheia CERTDIGITAL TSA G5 (RSA 3072, e = 65537) se generează în ceremonia G5, sub control multipersoană (M din N), cu proces-verbal, direct în modulul Thales Luna PCIe HSM 7 A790 (eIDAS-2400055-01), în partiția SVG5; certificatul ei este emis de CERTDIGITAL QCA G5 (DPC CERTDIGITAL G5, secțiunea 6.1.1).

11.6.2. Protecția cheii private a TSU

Cheia privată este păstrată și utilizată numai în HSM. Pentru CERTDIGITAL TSA G4, copia de rezervă este criptată cu cheia master a HSM (MBK) și poate fi restaurată numai într-un HSM certificat, sub control dual (M din N); pentru CERTDIGITAL TSA G5, copia de rezervă se realizează

prin clonarea criptată a partiției SVG5 în al doilea modul Thales Luna PCIe HSM 7 A790, sub control multipersoană (M din N), cu proces-verbal (DPC CERTDIGITAL G5, secțiunea 6.2.4).

11.6.3. Certificatul TSU

Element	Valoare
Subiect	C=RO, O=CENTRUL DE CALCUL S.A., OU=CERTDIGITAL, organizationIdentifier=VATRO-2163993, CN=CERTDIGITAL TSA G4
Emitent	CERTDIGITAL QUALIFIED CA G4
Valabilitate	18.07.2023 – 07.07.2038
Cheie	RSA 4096
Politici	QCP-l-qscd (0.4.0.194112.1.3), 1.3.6.1.4.1.47898.4.2.2.1.2
keyUsage / extKeyUsage	digitalSignature, nonRepudiation (critic) / timeStamping (critic)
qcStatements	QcCompliance, QcSSCD, QcType eSeal, QcPDS

Certificatul este publicat la https://certs.certdigital.ro/certdigital_tsa_g4.crt.

Pentru CERTDIGITAL TSA G5:

Element	Valoare
Subiect	C=RO, O=CENTRUL DE CALCUL S.A., OU=CERTDIGITAL, organizationIdentifier=VATRO-2163993, CN=CERTDIGITAL TSA G5
Emitent	CERTDIGITAL QCA G5
Valabilitate	3 ani de la emitere; cheia se utilizează cel mult 2 ani (secțiunea 11.6.4)
Cheie / semnătura emitentului	RSA 3072, e = 65537 / sha512WithRSAEncryption
Politici	QCP-l-qscd (0.4.0.194112.1.3), 1.3.6.1.4.1.47898.5.2.2.1.2
keyUsage / extKeyUsage	digitalSignature, nonRepudiation (critic) / timeStamping (critic)
qcStatements	QcCompliance, QcSSCD, QcType eSeal, QcPDS (en, ro), semanticsId-Legal (0.4.0.194121.1.2)
CRL / OCSP / certificatul emitentului	http://crl.certdigital.ro/certdigital_qualified_g5.crl / http://ocsp.g5.certdigital.ro / http://certs.certdigital.ro/certdigital_qualified_g5.crt

Certificatul CERTDIGITAL TSA G5 se publică la http://certs.certdigital.ro/certdigital_tsa_g5.crt.

11.6.4. Reînnoirea cheii TSU

Cheia TSU se înlocuiește înaintea sfârșitului perioadei de utilizare (07.07.2035), cu cheia și certificatul CERTDIGITAL TSA G5 (RSA 3072; certificatul este valabil 3 ani, iar cheia se utilizează cel mult 2 ani de la emitere, conform ETSI EN 319 421, TIS-7.6.7-04), generate în ceremonie. ADR este informată cu cel puțin o lună înainte. După înlocuire, certificatul CERTDIGITAL TSA G4 rămâne publicat la https://certs.certdigital.ro/certdigital_tsa_g4.crt, pentru verificarea mărcilor emise până atunci, iar pe durata tranziției ambele certificate, CERTDIGITAL TSA G4 și CERTDIGITAL TSA G5, figurează ca identități ale serviciului în Lista de încredere.

11.6.5. Ciclul de viață al hardware-ului criptografic

HSM-ul este achiziționat de la producător, verificat la recepție, instalat în zona de securitate și administrat sub control dual; firmware-ul se actualizează numai cu versiuni certificate, cu proces-verbal.

11.6.6. Sfârșitul ciclului de viață al cheii TSU

După încetarea utilizării, cheia TSU și copiile ei se distrug prin zeroizare, cu proces-verbal, iar certificatul se revocă dacă nu a expirat.

11.7. Marcarea temporală

11.7.1. Emiterea mărcii

Fiecare marcă conține un număr de serie unic, identificatorul politicii 0.4.0.2023.1.1, data și ora UTC, precizia de 1 s, amprenta primită și declarația esi4-qtstStatement-1. TSU nu emite mărci dacă ceasul nu este sincronizat în limita de precizie.

11.7.2. Sincronizarea ceasului cu UTC

TSU se sincronizează prin NTP cu sursele descrise în documentul 00u: două servere de timp GNSS, câte unul în fiecare centru de date (sursa preferată și cea alternativă), și o sursă independentă de GNSS (NIST). Clientul NTP nu se consideră sincronizat dacă dispune de mai puțin de două surse concordante. Abaterea se monitorizează continuu, cu alertare în sistemul centralizat de jurnalizare; la depășirea preciziei, emiterea se oprește, evenimentul se înregistrează și se tratează ca incident. Secundele intercalare se tratează conform sursei de timp.

11.8. Securitatea fizică și a mediului

TSU și HSM-ul sunt amplasate în zona de securitate a centrului de date principal, cu acces controlat prin autentificare în mai mulți factori; centrul de date secundar găzduiește echipamentele de rezervă (PG, cap. 8).

11.9. Securitatea operațiunilor

Modificările se fac prin procedura de gestionare a schimbărilor; vulnerabilitățile se remediază în funcție de criticitate; protecția împotriva programelor malițioase este activă.

Sistemul de operare al serverului TSU este o versiune suportată de producător, cu actualizările de securitate aplicate.

11.10. Securitatea rețelei

TSU este într-o zonă de rețea dedicată. Sunt permise numai porturile necesare serviciului: HTTPS pentru RFC 3161, NTP către sursele de timp și administrarea din rețeaua internă dedicată; SMTP numai în ieșire, pentru alerte.

11.11. 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, DNSC (entitate esențială nr. E-210D02), ANSPDCP în 72 de ore dacă sunt afectate date cu caracter personal, persoanele afectate. La compromiterea cheii TSU sau la pierderea sincronizării care afectează mărcile emise, CERTDIGITAL oprește emiterea, revocă certificatul TSU, informează abonații și părțile care se bazează și publică informațiile necesare identificării mărcilor afectate.

11.12. Colectarea dovezilor

Se înregistrează: cererile și mărcile emise (număr de serie, ora, amprenta), evenimentele de sincronizare și de alarmă ale ceasului, evenimentele privind cheia TSU și HSM-ul, accesul administrativ. Jurnalele se păstrează cel puțin 10 ani de la data înregistrării, protejate împotriva modificării.

11.13. Continuitatea activității

Serviciul se restabilește în cel mult 8 ore, conform Procedurii de continuitate operațională și de recuperare în caz de dezastru (PO/SI/63); jurnalele se replică în centrul de date secundar la cel mult 5 minute. CERTDIGITAL nu operează o TSU de rezervă activă; la comutare, emiterea se reia numai după verificarea sincronizării cu UTC.

11.14. Încetarea TSA

Încetarea serviciului se face conform Planului de încetare a serviciilor (00r): ADR este informată cu cel puțin 3 luni înainte (în 24 de ore la încetarea neprevăzută); abonații și părțile care se bazează sunt informați; cheia TSU se distruge pe bază de proces-verbal; certificatul TSU se revocă; înregistrările se păstrează 10 ani prin custode.

11.15. Conformitatea

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; ADR, organismul de supraveghere, este informată cu cel puțin o lună înainte, iar raportul se transmite ADR în cel mult 3 zile lucrătoare. Datele cu caracter personal (datele de cont ale abonaților și jurnalele tehnice) se prelucrează conform Regulamentului (UE) 2016/679 și Politicii de protecție a datelor (00d); serviciul prelucrează numai amprentele datelor.