



Politica Serviciilor de Încredere pentru Marca Temporală

EMISA DE:

DEPARTAMENT	NUME	DATA
MANAGEMENTUL POLITICILOR SI PROCEDURILOR	DIRECTOR TEHNIC	09.04.2012

APROBATA DE:

DEPARTAMENT	NUME	DATA
CERTIFICATE CALIFICATE	DIRECTOR TEHNIC	09.04.2012

ISTORICUL MODIFICARILOR:

VERSIUNE	AUTOR	DETALII MODIFICARI	DATA:
1.0.0	SEF COMPARTIMENT	Prima versiune a documentului	09.04.2012
1.1	DIRECTOR TEHNIC	Modificari conform Regulamentului (EU) 910/2014	08.05.2017
1.2	DIRECTOR TEHNIC	Revizuire document	31.01.2019
1.3	DIRECTOR TEHNIC	Revizuire document	30.06.2019
1.4	DIRECTOR TEHNIC	Revizuire document	31.01.2020
1.5	DIRECTOR TEHNIC	Revizuire document	31.01.2021

1.6	DIRECTOR TEHNIC	Adăugare autorități CERTDIGITAL G4	30.06.2023
1.7	CERTDIGITAL	Actualizare document in conformitate cu Legea 214/2014	06.10.2025

Cuprins

1. Introducere	5
1.1. Marca CertDigital	5
1.2. Conținut	5
2. Politica de marcare temporală	7
2.1. Marcarea temporală	7
2.2. Autoritatea de marcare temporală	7
2.3. Obligații	8
2.3.1. Obligațiile Autorității de Marcare Temporală	8
2.3.2. Obligațiile utilizatorului	10
2.4. Răspunderi	11
2.5. Confidențialitatea	13
2.6. Drepturile de proprietate intelectuală	14
3. Managementul ciclului de viață al cheii	20
3.1. Generarea cheii TSA	20
3.2. Protecția cheilor private TSA	20
3.2.1. Standarde pentru modulele criptografice	20
3.2.2. Controlul multi-persoane al accesului cheii private	20
3.2.3. Intrarea unei chei private în modulul criptografic	20
3.2.4. Activarea cheilor private	21
3.2.5. Dezactivarea cheilor private	21
3.3. Distribuția cheilor publice TSA	21
3.4. Distrugerea cheii private	22
3.5. Managementul modulului hardware de securitate	22
3.6. Sincronizarea cu baza de timp	22
3.7. Structura Marcii Temporale	23
3.8. Profilul certificatului	24
4. Registrul Electronic Operativ de evidență al mărcilor temporale	26
5. Actualizarea politicii	27

1. Introducere

1.1. Marca CertDigital

CertDigital reprezintă marca sub egida căreia Centrul de Calcul S.A. furnizează serviciile de încredere pentru certificare și de marcă temporală. De fiecare dată când în conținutul acestui document se fac referiri la CertDigital, acele referiri implică compania Centrul de Calcul S.A.

1.2. Conținut

Documentul „Politica Serviciilor de Marcă Temporală” definește practicile și procedurile de lucru implementate de CertDigital în calitate de furnizor de servicii de marcă temporală în baza Regulamentului (UE) nr. 910/2014 și a Legii 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea.

Prin natura serviciilor prestate, CertDigital asigură confidențialitatea prelucrării datelor personale ale clienților printr-o declarație de confidențialitate agreată de către părți.

Acest document include printre practicile și procedurile de lucru definite aspecte precum:

- Obligațiile și responsabilitățile autorității de marcă temporală, respectiv ale utilizatorilor de servicii de marcă temporală;
- Aspectele juridice privind furnizarea serviciilor de încredere pentru marcă temporală de către CertDigital;
- Managementul ciclului de viață al cheilor

- Modalitatea de administrare a Politicii Serviciilor de Marcare Temporală.

Descrierea detaliată a practicilor și procedurilor privind serviciile de marcă temporală este prezentată în Declarația Practicilor Serviciilor de Marcă Temporală (DPSMT).

Cunoașterea Politicii Serviciilor de Marcă Temporală, precum și a Declarației Practicilor Serviciilor de Marcă Temporală prezintă importanță în mod special pentru abonații și entitățile partener ale CertDigital.

2. Politica de marcare temporală

2.1. Marcarea temporală

Prin serviciul de marcare temporală, CertDigital furnizează:

- Servicii de încredere pentru generarea mărcii temporale;
- Servicii de control al calității serviciilor de încredere pentru marcare temporală pentru îndeplinirea standardelor de calitate prestabilite prin prezentul document.

În cadrul procesului de marcare temporală, utilizatorul transmite către CertDigital o cerere de emitere a mărcii temporale pentru un anumit document electronic. Această cerere conține amprenta digitală a documentului pentru care se face cererea, amprenta creată prin intermediul aplicării unei funcții hash-code asupra documentului. CertDigital aplică informația de timp, raportându-se la baza de timp și semnează electronic utilizând un certificat digital calificat, rezultând marca temporală ce este transmisă utilizatorului.

2.2. Autoritatea de marcare temporală

Prin îndeplinirea reglementărilor aferente Regulamentului (UE) nr. 910/2014 și ale Legii 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, CertDigital își definește cadrul de a furniza servicii de marcare temporală către abonati și își asumă răspunderea deplină asupra furnizării acestor servicii.

CertDigital generează și semnează marcile temporale printr-un server TSA (Time Stamp Authority).

Sistemul informatic implementat de către CertDigital permite

furnizarea continua a serviciilor de marcare temporală și asigură faptul că este imposibil să fie emisă o marcă corectă pentru un alt timp decât momentul când a fost primit documentul sau să se schimbe ordinea în care marcele de timp sunt emise.

2.3. Obligații

2.3.1. Obligațiile Autorității de Marcare Temporală

Printr-o politică asumată și pusă la dispoziția utilizatorilor, autoritatea de marcare temporală CertDigital își atribuie o serie de obligații fundamentale după cum urmează:

- Constituirea unui document (în speta, Politica Serviciilor de Marcare Temporală) prin intermediul căruia să se definească modalitatea de lucru, procedurile aplicabile, politica generală a Companiei, obligațiile și drepturile partilor contractante, etc care să fie aprobat de conducere și publicat într-un mediu accesibil utilizatorilor cărora i se adresează;
- Desfășurarea activității în conformitate cu procedurile descrise în prezentul document;
- Implementarea unor resurse hardware și software fiabile care să susțină buna desfășurare a activității în mod permanent în baza reglementărilor impuse, dar și din punct de vedere al afacerilor în mediul virtual;
- Generarea unei perechi funcționale cheie privată - cheie publică și protecția cheii private prin utilizarea unui dispozitiv criptografic securizat, cu adoptarea măsurilor necesare pentru a preveni pierderea, dezvăluirea, modificarea sau utilizarea neautorizată a cheii private ce este folosită exclusiv în scopul aplicării semnăturii electronice asupra mărcilor temporale emise;

- Crearea și menținerea unui registru electronic operativ de evidență a mărcilor temporale incluzând momentul de timp la care au fost emise mărcile temporale;
- Punerea la dispoziția utilizatorilor software-ul necesar pentru utilizarea serviciului de marcare temporală și informațiile legate de: condițiile în care este disponibil software-ul, instrucțiunile de folosire, obligațiile utilizatorului sau orice alte limitări privind utilizarea software-ului;
- Alocarea de personal ce detine cunoștințe de specialitate, experiență și calificare necesare pentru furnizarea serviciilor de marcare temporală;
- Menținerea pe o perioadă de 10 ani a înregistrărilor mărcilor temporale;
- Păstrarea documentației aferente algoritmilor și procedurilor de generare a mărcilor temporale emise;
- Punerea la dispoziție a unui serviciu gratuit de verificare on-line a mărcilor temporale;
- Asigurarea accesului permanent la baza de timp;
- Informarea utilizatorilor privind termenii și condițiile care privesc utilizarea serviciilor de marcare temporală. În acest sens, CertDigital pune la dispoziția utilizatorilor prin intermediul site-ului propriu <https://www.certdigital.ro>, următoarele informații:
 - datele de contact CertDigital;
 - politica de marcare temporală aplicată;
 - standardele tehnice aplicabile;
 - precizia timpului din mărcile temporale;

- limitările în folosirea serviciului de marcă temporală;
- obligațiile utilizatorului;
- informații despre cum trebuie verificată marca temporală și limitări posibile asupra perioadei de valabilitate;
- informații privind protecția datelor cu caracter personal;
- perioada de timp în care sunt păstrate înregistrările referitoare la evenimente ale CertDigital;
- Asigurarea protecției datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR, precum și cu Legea nr. 506/2004 (actualizată) privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (inclusiv regulile privind comunicațiile electronice și cookie-urile).;
- Informarea utilizatorilor asupra obligațiilor pe care le dețin în baza acestui document, dar și asupra riscului la care se supun prin nerespectarea acestor obligații;
- În cazul încetării activității, furnizorul de servicii de marcă temporală CertDigital se obligă să transfere unui alt furnizor de servicii de marcă temporală sau, după caz, autorității registrul electronic operativ de evidență, registrul mărcilor temporale, precum și documentația aferentă algoritmilor și procedurilor de generare a mărcilor temporale emise.

2.3.2. Obligațiile utilizatorului

Documentul de față reprezintă parte integrantă în contractul dintre Furnizorul de Servicii de Marcă Temporală și utilizatorul acestor servicii. Astfel, pe baza acestui contract, utilizatorul își exprimă acordul asupra normelor specificate prin acest document și se

supune următoarelor obligații:

- Supunerea la regulile si procedurile descrise in prezentul document.
- Furnizarea informațiilor referitoare la identitatea sa.
- Utilizarea aplicației de marcare temporală pusă la dispoziție de către CertDigital.
- Autentificarea marcii temporale obtinute prin verificarea semnăturii digitale CertDigital. CertDigital detine certificatul corespunzator cheii publice, pe baza caruia se verifica semnatura asupra marcii temporale.
- Verificarea increderii si a validitatii certificatului cu care a fost semnata marca.

2.4. Răspunderi

În concordanță cu reglementările referitoare la răspunderea furnizorilor de servicii de marcare din Regulamentul (UE) nr. 910/2014 și din Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, CertDigital, în calitate de Furnizor al Serviciilor de Marcare Temporală, răspunde pentru prejudiciul adus oricărei persoane care își întemeiază conduita pe efectele juridice ale respectivelor mărci temporale:

- în ceea ce privește exactitatea, în momentul eliberării marcii temporale, a tuturor informațiilor pe care le conține;
- în ceea ce privește asigurarea ca, în momentul eliberării marcii temporale, furnizorul identificat în cuprinsul acesteia detinea datele de generare a marcii temporale corespunzătoare datelor de verificare a marcii temporale, prevăzute în prezenta lege;

- in privinta indeplinirii tuturor obligatiilor prevazute la capitolul 2.3.1.

Furnizorul de servicii de marcare temporală CertDigital trebuie sa dispună de instrumente financiare asiguratorii pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfășurării activităților legate de marcarea temporală.

CertDigital nu răspunde pentru prejudiciile rezultate din utilizarea unei mărci temporale cu încălcarea restricțiilor prevăzute in cuprinsul acesteia.

2.5. Confidențialitatea

Informațiile din posesia CertDigital sunt obținute, stocate și procesate în conformitate cu Legea 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice și a altor reglementări legale în vigoare, REGULAMENTUL nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

În prestarea serviciilor de încredere CERTDIGITAL prelucrează date cu caracter personal ale Subiectului/Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiilor de drept intern, a Regulamentului nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor. Scopul prelucrării datelor cu caracter personal este acela de a presta servicii de certificare.

Utilizarea și prelucrarea datelor persoanele de către CertDigital se realizează strict în măsura în care aceasta activitatea este necesară serviciilor de marcare temporală.

CertDigital asigură toate măsurile de protecție împotriva accesului neautorizat asupra datelor personale.

2.6. Drepturile de proprietate intelectuală

Prezenta politică reprezintă proprietatea intelectuală a CertDigital.

CertDigital deține toate drepturile de proprietate intelectuală asupra certificatelor calificate emise de aceasta, iar reproducerea certificatelor este permisă exclusiv cu acordul CertDigital.

Perechile de chei corespunzătoare certificatelor Autorității de Certificare calificate CertDigital reprezintă proprietatea CertDigital.

Perechile de chei corespunzătoare certificatelor semnatarilor sunt proprietatea semnatarilor specificați în aceste certificate.

3. Managementul ciclului de viață al cheii

3.1. Generarea cheii TSA

Cheile TSA sunt generate în cadrul unui modul hardware de securitate în conformitate cu standardul NIST FIPS 140-1 Nivel 3 de către personalul de încredere cu funcții definite de încredere.

Cheia privată nu poate fi dedusă în niciun fel din cheia sa publică pereche.

3.2. Protecția cheilor private TSA

3.2.1. Standarde pentru modulele criptografice

CertDigital folosește module criptografice care sunt certificate FIPS 140-1 Nivel 3 și îndeplinesc standardele industriale pentru generarea de numere aleatorii.

Cheile utilizate de către Autoritatea de Marcare Temporală CertDigital sunt generate și stocate în module de securitate hardware (HSM) ce pot fi activate simultan doar de două persoane și care, de asemenea, este validat FIPS 140-1 Nivel 3.

3.2.2. Controlul multi-persoane al accesului cheii private

Serviciile CertDigital folosesc module hardware care necesită implicarea mai multor persoane pentru a îndeplini sarcini sensibile. Toate instrumentele necesare realizării acestor operațiuni sunt stocate în siguranță și nu pot fi accesate fără informațiile deținute de către persoanele autorizate.

3.2.3. Intrarea unei chei private în modulul criptografic

Cheile private CertDigital se generează și se stochează pe modulele

de securitate hardware validate FIPS 140-1 Nivel 3, în care, de altfel, vor fi folosite.

3.2.4. Activarea cheilor private

Activarea cheilor private CertDigital emise presupune autentificarea prin parola și/ sau PIN.

Utilizatorii sunt singurii responsabili pentru protecția cheilor private pe care le au în posesie. CertDigital nu deține nicio responsabilitate în generarea, protejarea sau distribuirea acestor chei.

CertDigital sugerează utilizatorilor săi autentificarea folosirea parole puternice pentru a preveni accesul neautorizat și folosirea frauduloasă a cheilor private.

3.2.5. Dezactivarea cheilor private

Cheile private stocate pe un modul de securitate hardware sunt dezactivate odată cu scoaterea cardului din dispozitiv.

În cazul unui utilizator, dezactivarea cheii primare se realizează la ieșirea din aplicația, când, de fapt, se închide sesiunea de lucru.

În timpul utilizării, modulele de securitate hardware nu trebuie lăsate nesupravegheate sau în oricare altă stare care ar putea favoriza accesul neautorizat. Când nu sunt folosite, modulele trebuie depozitate într-o locație încuiată ce beneficiază de un grad sporit de securitate.

3.3. Distribuția cheilor publice TSA

Cheile publice corespundente certificatelor TSA sunt publicate pe site-ul CertDigital la adresa: <https://ca.certdigital.ro/tsa/>

3.4. Distrugerea cheii private

În forma inițială, distrugerea cheii primare presupune ștergerea ei de pe mediul de stocare într-o manieră care să asigure faptul că nu au rămas fragmente ale cheii care ar putea permite reconstituirea ei.

Modulele de Securitate Hardware (primare și cele de back-up) sunt reinițializate în conformitate cu specificațiile producătorului de hardware. În cazul în care, această procedură eșuează, CertDigital își asumă obligația de a distruge echipamentele într-o mod care să nu permită recuperarea cheii private.

3.5. Managementul modului hardware de securitate

Aferent modului hardware de securitate, Autoritatea de Marcare Temporală CertDigital aplică următoarele controale:

- Verificarea sigiliilor de securitate la livrarea echipamentului;
- Stocarea echipamentului într-un spațiu securizat cu acces limitat persoanelor autorizate;
- Realizarea instalării și a inițierii de către persoane de încredere;
- Ștergerea și distrugerea cheilor în conformitate cu recomandările producătorului în cazul scoaterii din funcțiune.

3.6. Sincronizarea cu baza de timp

Furnizorul de servicii de încredere pentru marcă temporală CertDigital obține și menține referința de timp trasabilă la UTC din surse redundante (NTP/PTS) de nivel stratum-1, inclusiv servere din NTP Pool (ex. ro.pool.ntp.org) și furnizori internaționali consacrați (de tip NIST, PTB sau echivalenți), precum și, după caz, din servere locale disciplinate GNSS (GPS/GLONASS/Galileo).

Sursa de timp utilizată de CertDigital este sincronizată astfel încât abaterea față de UTC să nu depășească ± 1 secundă. În acest scop, CertDigital implementează măsuri de calibrare periodică, monitorizare continuă (drift/offset/jitter), alarme la depășirea pragurilor, mecanisme de failover între surse și auditare a sincronizării, pentru a asigura respectarea permanentă a pragului de acuratețe menționat.

3.7. Structura Marcii Temporale

Marca temporală folosită are următoarea structură:

A. Informații despre marca temporală propriu-zisă

- Versiune
- Politică
- Amprenta de marcat
- Număr serial unic
- Momentul exact de timp al emiterii

B. Semnatura furnizorului

- Info semnatura

C. Statutul PKI

- Codul de status PKI

3.8. Profilul certificatului

Profilul unui certificat de cheie publica care este utilizat de Autoritatea de Marcare Temporală respecta recomandările IETF din RFC 3161 și este de următoarea formă:

Numele campului	Valoare sau valoare limita	
Versiunea	Versiunea 3	
Numarul serial	Valoare unica pentru fiecare certificat emis	
Algoritmul de semnatura	Obiect identificator al algoritmului utilizat pentru semnarea certificatului (functia hash- code SHA-256/ SHA-512 si algoritmul de criptare RSA)	
Emitentul (Numele distinctiv)	Common Name (CN)=	
	Organization Identifier (2.5.4.97) =	
	Organization Unit Name (OU) =	
	Organization (O) =	
	Country (C) =	
Nu inainte de (data de incepere a valabilitatii):	Data de incepere a validitatii certificatului identificata pe baza sincronizarii serverului cu ora oficiala a Romania	

Nu după (data expirării)	Data de expirare a validității certificatului identificată pe baza sincronizării serverului cu ora oficială a României. Valabilitatea certificatelor se stabilește în concordanță cu prevederile obligatorii.
Subiectul (Numele distinctiv)	Numele distinctiv respectă cerințele standardului X.509 v.3. Anumite atribute din componenta Numelui Distinct pot avea caracter opțional.
Informații despre cheia publică a subiectului	Codificate în conformitate cu RFC 2459 Oferă informații despre cheile publice RSA. Mărimea cheii este de 2048 biți.
Semnatura	Generată și codificată în concordanță cu RFC 2459
Enhanced Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
Qualified Certificate Statements	esi4-qcStatement-1: 0.4.0.1862.1.1 esi4-qcStatement-4: 0.4.0.1862.1.4 esi4-qcStatement-6: 0.4.0.1862.1.6 id-etsi-qcs-QcType 1: 0.4.0.1862.1.6.2 esi4-qcStatement-5: 0.4.0.1862.1.5

4. Registrul Electronic Operativ de evidenta al mărcilor temporale

CertDigital menține un Registru Electronic Operativ de evidenta a mărcilor temporale incluzând momentul de timp la care au fost emise mărcile temporale, in conformitate cu cerințele Legii 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea.

Acest registru evidențiază toate mărcile temporale emise de către Furnizorul de Servicii de Încredere pentru Marcare Temporală CertDigital, si cuprinde, pe lângă marca temporală propriu-zisă, si date referitoare la marca temporală si la certificatul utilizat. De asemenea, in cadrul registrului de evidenta CertDigital include înregistrări ale evenimentelor apărute in sistemul informatic utilizat pentru generarea mărcilor temporale. Acest registru este disponibil permanent pentru consultare pe pagina web CertDigital: <https://ca.certdigital.ro/tsa/>.

Toate aceste informații referitoare la Registrul Electronic Operativ de evidenta al mărcilor temporale sunt păstrate pe o perioada de minimum 10 ani.

5. Actualizarea politicii

Politica Serviciilor de Încredere pentru Marcare Temporală CertDigital se poate modifica periodic. Aceste modificări vor fi disponibile tuturor abonaților prin intermediul site-lui Web al CertDigital. Abonații care nu acceptă modificările aduse Politicii Serviciilor de Marcare Temporală trebuie să trimită către CertDigital o declarație în acest sens și să renunțe la serviciile oferite de CertDigital.