Politica Serviciilor de Marcare Temporala

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

Cuprins

1. Introducere

1.1. Marca CertDigital

CertDigital reprezinta marca sub egida careia Centrul de Calcul S.A. furnizeaza serviciile de certificare si de marcare temporala. De fiecare data cand in continutul acestui document se fac referiri la CertDigital, acele referiri implica compania Centrul de Calcul S.A.

1.2. Continut

Documentul „Politica Serviciilor de Marcare Temporala" defineste practicile si procedurile de lucru implementate de CertDigital in calitate de furnizor de servicii de marcare temporala in baza Regulamentului (UE) nr. 910/2014 si a Legii nr. 451/2004 privind marca temporala, in scopul furnizarii serviciilor de marcare temporala.

Prin natura serviciilor prestate, CertDigital asigura confidentialitatea prelucrarii datelor personale ale clientilor printr-o declaratie de confidentialitate agreata de catre parti.

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

- Obligatiile si responsabilitatile autoritatii de marcare temporala, respectiv ale utilizatorilor de servicii de marcare temporala;
- Aspectele juridice privind furnizarea serviciilor de marcare temporala de catre CertDigital;
- Managementul ciclului de viata al cheilor
- Modalitatea de administrare a Politicii Serviciilor de Marcare Temporala.

Descrierea detaliata a practicilor si procedurilor privind serviciile de marcare temporala este prezentata în Declaratia Practicilor Serviciilor de Marcare Temporala (DPSMT).

Cunoaşterea Politicii Serviciilor de Marcare Temporala, precum şi a Declaratiei Practicilor Serviciilor de Marcare Temporala prezintă importanţă în mod special pentru abonaţii şi entităţile partener ale CertDigital.

2. Politica de marcare temporala

2.1. Marcarea temporala

Prin serviciul de marcare temporala, CertDigital furnizeaza:

- Servicii de generare a marcii temporale;
- Servicii de control al calitatii serviciilor de marcare temporala pentru indeplinirea standardelor de calitate prestabilite prin prezentul document.

In cadrul procesului de marcare temporala, utilizatorul transmite catre CertDigital o cerere de emitere a marcii temporale pentru un anumit document electronic. Aceasta cerere contine amprenta digitala a documentului pentru care se face cererea, amprenta creata prin intermediul aplicarii unei functii hash-code asupra documentului. CertDigital aplica informatia de timp, raportandu-se la baza de timp si semneaza electronic utilizand un certificat digital calificat, rezultand marca temporala ce este transmisa utilizatorului.

2.2. Autoritatea de marcare temporala

Prin indeplinierea reglementarilor aferente Regulamentului (UE) nr. 910/2014 si ale Legii nr. 451/2004 privind marca temporala si a normelor sale aplicabile, CertDigital isi defineste cadrul de a furniza servicii de marcare temporala catre abonati si isi asuma raspunderea deplina asupra furnizarii acestor servicii.

CertDigital genereaza si semneaza marcile temporale printr-un server TSA (Time Stamp Authority).

Sistemul informatic implementat de catre CertDigital permite furnizarea continua a serviciilor de marcare temporala si asigura

faptul ca este imposibil sa fie emisa o marca corecta pentru un alt timp decat momentul cand a fost primit documentul sau sa se schimbe ordinea in care marcile de timp sunt emise.

2.3. Obligatii

2.3.1. Obligatiile Autoritatii de marcare temporala

Printr-o politica asumata si pusa la dispozitia utilizatorilor, autoritatea de marcare temporala CertDigital isi atribuie o serie de obligatii fundamentale dupa cum urmeaza:

- Constituirea unui document (in speta, Politica Serviciilor de Marcare Temporala) prin intermediul caruia sa se defineasca modalitatea de lucru, procedurile aplicabile, politica generala a Companiei, obligatiile si drepturile partilor contractante, etc care sa fie aprobat de catre Conducere si publicat intr-un mediu accesibil utilizatorilor carora i se adreseaza;
- Desfasurarea activitatii in conformitate cu procedurile descrise in prezentul document;
- Implementarea unor resurse hardware si software fiabile care sa sustina buna desfasurare a activitatii in mod permanent in baza reglementarilor impuse, dar si din punct de vedere al afacerilor in mediul virtual;
- Generarea unei perechi functionale cheie privata - cheie publica si protectia cheii private prin utilizarea unui dispozitiv criptografic securizat, cu adoptarea masurilor necesare pentru a preveni pierderea, dezvaluirea, modificarea sau utilizarea neautorizata a cheii private ce este folosita exclusiv in scopul aplicarii semnaturii electronice asupra marcilor temporale emise;

- Crearea si mentinerea un registru electronic operativ de evidenta a marcilor temporale incluzand momentul de timp la care au fost emise marcile temporale;
- Punerea la dispozitia utilizatorilor software-ul necesar pentru utilizarea serviciului de marcare temporala si informatiile legate de: conditiile in care este disponibil software-ul, instructiunile de folosire, obligatiile utilizatorului sau orice alte limitari privind utilizarea software-ului;
- Alocarea de personal ce detine cunostinte de specialitate, experienta si calificare necesare pentru furnizarea serviciilor de marcare temporala;
- Mentinerea pe o perioada de 10 ani a inregistrarilor marcilor temporale;
- Pastrarea documentatiei aferente algoritmilor si procedurilor de generare a marcilor temporale emise;
- Punerea la dispozitie a unui serviciu gratuit de verificare on-line a marcilor temporale;
- Asigurarea accesului permanent la baza de timp;
- Informarea utilizatorilor privind termenii si conditiile care privesc utilizarea serviciilor de marcare temporala. In acest sens, CertDigital pune la dispozitia utilizatorilor prin intermediul site-ului propriu https://www.certdigital.ro, urmatoarele informatii:
    - datele de contact CertDigital;
    - politica de marcare temporala aplicata;
    - standardele tehnice aplicabile;
    - precizia timpului din marcile temporale;

- limitarile in folosirea serviciului de marcare temporala;
- obligatiile utilizatorului;
- informatii despre cum trebuie verificata marca temporala si limitari posibile asupra perioadei de valabilitate;
- informatii privind protectia datelor cu caracter personal;
- perioada de timp in care sunt pastrate inregistrarile referitoare la evenimente ale CertDigital;

- Asigurarea protectiei datelor cu caracter personal in concordanta cu Legea nr. 677/2001 privind protectia datelor cu caracter personal si cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice;
- Informarea utilizatorilor asupra obligatiilor pe care le detin in baza acestui document, dar si asupra riscului la care se supun prin nerespectarea acestor obligatii;
- In cazul incetarii activitatii, furnizorul de servicii de marcare temporala CertDigital se obliga sa transfere unui alt furnizor de servicii de marcare temporala sau, dupa caz, autoritatii registrul electronic operativ de evidenta, registrul marcilor temporale, precum si documentatia aferenta algoritmilor si procedurilor de generare a marcilor temporale emise.

2.3.2. Obligatiile utilizatorului

Documentul de fata reprezinta parte integranta in contractul dintre Furnizorul de Servicii de Marcare Temporala si utilizatorul acestor servicii. Astfel, pe baza acestui contract, utilizatorul isi exprima acordul asupra normelor specificate prin acest document si se supune urmatoarelor obligatii:

- Supunerea la regulile si procedurile descrise in prezentul document.
- Furnizarea informatiilor referitoare la identitatea sa.
- Utilizarea aplicatiei de marcare temporala pusa la dispozitie de catre CertDigital.
- Autentificarea marcii temporale obtinute prin verificarea semnaturii 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. Raspunderi

In concordanta cu reglementarile referitoare la raspunderea furnizorilor de servicii de marcare din Regulamentul (UE) nr. 910/2014 si din Legea nr. 451/2004 privind marca temporala, CertDigital, in calitate de Furnizor al Serviciilor de Marcare Temporala, raspunde pentru prejudiciul adus oricarei persoane care isi intemeiaza conduita pe efectele juridice ale respectivelor marci temporale:

- in ceea ce priveste exactitatea, in momentul eliberarii marcii temporale, a tuturor informatiilor pe care le contine;
- in ceea ce priveste asigurarea ca, in momentul eliberarii marcii temporale, furnizorul identificat in cuprinsul acesteia detinea datele de generare a marcii temporale corespunzatoare datelor de verificare a marcii temporale, prevazute in prezenta lege;
- in privinta indeplinirii tuturor obligatiilor prevazute la capitolul 2.3.1.

Furnizorul de servicii de marcare temporala CertDigital trebuie sa dispuna de instrumente financiare asiguratorii pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfasurarii activitatilor legate de marcarea temporala.

CertDigital nu raspunde pentru prejudiciile rezultate din utilizarea unei marci temporale cu incalcarea restrictiilor prevazute in cuprinsul acesteia.

2.5. Confidentialitatea

Informatiile din posesia CertDigital sunt obtinute, stocate si procesate in conformitate cu Legea 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date, Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice si a altor reglementari legale in vigoare.

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 dispozițiile de drept intern, a Regulamentului nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie 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 si prelucrarea datelor persoanale de catre CertDigital se realizeaza strict in masura in care aceasta activitatea este necesara serviciilor de marcare temporala.

CertDigital asigura toate masurile de protectie impotriva accesului neautorizat asupra datelor personale.

2.6. Drepturile de proprietate intelectuala

Prezenta politica reprezinta proprietatea intelectuala a CertDigital.

CertDigital detine toate drepturile de proprietate intelectuala asupra certificatelor calificate emise de aceasta, iar reproducerea certificatelor este permisa exclusiv cu acordul CertDigital.

Perechile de chei corespunzatoare certificatelor Autoritatii de

Certificare calificate CertDigital reprezinta proprietatea CertDigital.

Perechile de chei corespunzatoare certificatelor semnatarilor sunt proprietatea semnatarilor specificati in aceste certificate.

3. Managementul ciclului de viata al cheii

3.1. Generarea cheii TSA

Cheile TSA sunt generate in cadrul unui modul hardware de securitate in conformitate cu standardul NIST FIPS 140-1 Nivel 3 de catre personalul de incredere cu functii definite de incredere.

Cheia privata nu poate fi dedusa in niciun fel din cheia sa publica pereche.

3.2. Protectia cheilor private TSA

3.2.1. Standarde pentru modulele criptografice

CertDigital foloseste module criptografice care sunt certificate FIPS 140-1 Nivel 3 si indeplinesc standardele industriale pentru generarea de numere aleatorii.

Cheile utilizate de catre Autoritatea de Marcare Temporala CertDigital sunt generate si stocate in module de securitate hardware (HSM) ce pot fi activate simultan doar de doua persoane,si 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 necesita implicarea mai multor pesoane pentru a indeplini sarcini sensibile. Toate instrumentele necesare realizarii acestori operatiuni sunt stocate in siguranta si nu pot fi accesate fara informatiile detinute de catre persoanele autorizate.

3.2.3. Intrarea unei chei private in modulul criptografic

Cheile private CertDigital se genereaza si se stocheaza pe modulele

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

3.2.4. Activarea cheilor private

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

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

CertDigital sugereaza utilizatorilor sai autentificarea folosirea parole puternice pentru a preintampina accesul neautorizat si folosirea frauduloasa a cheilor private.

3.2.5. Dezactivarea cheilor private

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

In cazul unui utilizator, dezactivarea cheii primare se realizeaza la iesirea din aplicatia, cand, de fapt, se inchide sesiunea de lucru.

In timpul utilizarii, modulele de securitate hardware nu trebuie lasate nesupravegheate sau in oricare alta stare care ar putea favoriza accesul neautorizat. Cand nu sunt folosite, modulele trebuie depozitate intr-o locatie incuiata ce beneficiaza de un grad sporit de securitate.

3.3. Distributia cheilor publice TSA

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

3.4. Distrugerea cheii private

In forma initiala, distrugerea cheii primare presupune stergerea ei de pe mediul de stocare intr-o maniera care sa asigure faptul ca nu au ramas fragmente ale cheii care ar putea permite reconstituirea ei.

Modulele de Securitate Hardware (primare si cele de back-up) sunt reinitializate in conformitate cu specificatiile producatorului de hardware. In cazul in care, aceasta procedura esueaza, CertDigital isi asuma obligatia de a distruge echipamentele intr-o mod care sa nu permita recuperarea cheii private.

3.5. Managementul modulului hardware de securitate

Aferent modulului hardware de securitate, Autoritatea de Marcare Temporara CertDigital aplica urmatoarele controale:

- Verificarea sigiliilor de securitatea la livrarea echipamentului;
- Stocarea echipamentului intr-un spatiu securizat cu acces limitat persoanelor autorizate;
- Realizarea instalarii si a initierii de catre persoane de incredere;
- Stergerea si distrugerea cheilor in conformitate cu recomandarile producatorului in cazul scoaterii din functiune.

3.6. Sincronizarea cu baza de timp

Furnizorul de servicii de marcare temporala CertDigital utilizeaza informatia de timp a furnizorul unic de baza de timp si anume a Sistemului informatic pentru furnizarea orei oficiale a Romaniei, realizat de MCSI.

Sursa de timp folosita de catre CertDigital este sincronizata cu referinta de timp oferita de furnizorul unic de baza de timp cu o abatere maxima +/-1 secunda. In acest sens, CertDigital

implementeaza masuri de calibrare a echipamentelor astfel incat valoare abaterii mentionate sau nu fie depasita.

3.7. Structura Marcii Temporale

Marca temporala folosita are urmatoarea structura:

A. Informatii despre marca temporala propriu-zisa

- Versiune
- Politica
- Amprenta de marcat
- Numar 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 Temporala respecta recomandarile IETF din RFC 3161 si este de urmatoarea forma:

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 si algoritmul de criptare RSA)	
Emitentul (Numele distinctiv)	Numele (CN)=	
	Organizatia (O)=	
	Tara (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 dupa (data expirarii)	Data de expirare a validitatii certificatului identificata pe baza sincronizarii serverului cu ora oficiala a Romaniei. Valabilitatea certificatelor se stabileste in concordanta cu prevederile obligatorii.	

Subiectul (Numele distinctiv)	Numele distinctiv respecta cerintele standardului X.501. Anumite atribute din componenta Numelui Distinct pot avea caracter optional.
Informatii despre cheia publica a subiectului	Codificate in conformitate cu RFC 2459 Ofera informatii despre cheile publice RSA. Marimea cheii este de 2048 biti.
Semnatura	Generata si codificata in concordanta cu RFC 2459

4. Registrul Electronic Operativ de evidenta al marcilor temporale

CertDigital mentine un Registru Electronic Operativ de evidenta a marcilor temporale incluzand momentul de timp la care au fost emise marcile temporale, in conformitate cu cerintele Legii 451/2004 privind Marca Temporala si Normelor sale de aplicare. Acest registru evidentiaza toate marcile temporale emise de catre Furnizorul de Servicii de Marcare Temporala CertDigital, si cuprinde, pe langa marca temporala propriu-zisa, si date referitoare la marca temporala si la certificatul utilizat. De asemenea, in cadrul registrului de evidenta CertDigital include inregistrari ale evenimentelor aparute in sistemul informatic utilizat pentru generarea marcilor temporale. Acest registru este disponibil permanent pentru consultare pe pagina web CertDigital: https://ca.certidigital.ro/tsa/

Toate aceste informatii referitoare la Registrul Electronic Operativ de evidenta al marcilor temporale sunt pastrate pe o perioada de minimum 10 ani.

5. Actualizarea politicii

Politica Serviciilor de Marcare Temporala CertDigital se poate modifica periodic. Aceste modificări vor fi disponibile tuturor abonaţilor prin intermediul site-lui Web al CertDigital. Abonaţii care nu acceptă modificările aduse Politicii Serviciilor de Marcare Temporala trebuie să trimită către CertDigital o declaraţie în acest sens şi să renunţe la serviciile oferite de CertDigital.