



# **Politica de Certificare CertDigital**

<b>EMISA DE:</b>		
<b>DEPARTAMENT</b>	<b>NUME</b>	<b>DATA</b>
Manager Servicii Electronice	Manager Servicii Electronice	01.01.2016

<b>APROBATA DE:</b>		
<b>DEPARTAMENT</b>	<b>NUME</b>	<b>DATA</b>
Director General	Director General	01.06.2016

<b>ISTORICUL MODIFICARILOR:</b>			
<b>VERSIUNE</b>	<b>AUTOR</b>	<b>DETALII MODIFICARI</b>	<b>DATA:</b>
1.0.0	Director Tehnic	Publicarea primei versiuni	19.03.2011
1.0.1	Director Tehnic	Adaugarea noilor autoritati de certificare CertDigital Qualified CA Class 3 G2 CertDigital Enterprise CA Class 3 G2 CertDigital NonRepudiation CA Class 4 G2	01.06.2016

<b>LISTA DE DISTRIBUIRE:</b>	
<b>DESTINATAR</b>	<b>DATA</b>
Public - Internet	29.03.2011

## Cuprins

1. Introducere .....	4
2. Certificatele.....	4
2.1 Certificate de Clasă 1 .....	6
2.2 Certificate de Clasă 2 .....	7
2.3 Certificate de Clasă 3 .....	7
2.4 Certificate de Clasă 4 .....	9
3. Jetoane de ne-repudiere.....	10
3.1 Mărcile Temporale.....	10
3.2 Răspunsul de confirmare OCSP .....	11
4. Garantiile oferite de CertDigital.....	12
5. Acceptarea certificatului .....	12
6. Serviciul de certificare .....	12
7. Entitatea Partener.....	13
8. Abonatul .....	14
9. Actualizarea politicii de certificare .....	14
10. Taxe.....	14

## **1. Introducere**

Politica de Certificare a CertDigital (CP) descrie regulile și principiile generale aplicate de CertDigital în procesul de certificare a cheilor publice și folosire a autorității de marcare a timpului (TSA), precum și a altor servicii de ne-repudiare. Politica de certificare definește:

- entitățile implicate în procesele de certificare,
- responsabilitățile și obligațiile fiecărei entități,
- tipurile de certificate,
- tipurile de confirmări,
- procedurile de verificare a identității și
- aria de aplicabilitate.

Descrierea detaliată a regulilor de mai sus este prezentată în Codul de Practici și Proceduri (CPP).

Cunoașterea Politicii de Certificare, precum și al Codului de Practici și Proceduri prezintă importanță în mod special pentru abonații și entitățile partener ale CertDigital.

## **2. Certificatele**

Certificatul este un șir de date (mesaj) care conține cel puțin numele și identificatorul autorității, identificatorul abonatului, cheia sa publică, perioada de validitate, numărul serial și semnatura autorității emitente.

Certificatele sunt utilizate pentru a lega datele personale ale abonatului de cheile publice specifice. Proprietarul certificatului este, de asemenea, și proprietarul cheii private, corespunzătoare cheii publice conținută în certificat. Datele de identificare conținute în certificat permit altor părți să determine cu exactitate proprietarul certificatului. Dacă cheia privată este utilizată în timpul semnării electronice a unui mesaj, destinatarul mesajului poate fi sigur că mesajul a fost creat folosind

cheia privată, corespunzătoare cheii publice conținută în certificat (deci a fost creată de proprietarul certificatului) și mesajul nu a fost modificat de către altcineva.

Autoritatea de Certificare CertDigital CA confirmă prin emiterea unui certificat pentru un abonat:

- Identitatea acestuia sau credibilitatea altor date, ca de exemplu adresa căsuței de poștă electronică;
- Cheia publică conținută de certificat aparține abonatului respectiv.

Datorită celor de mai sus, entitățile partener, după recepția unui mesaj semnat, pot determina cine este proprietarul certificatului care a semnat mesajul și, opțional, îl pot trage pe acesta la răspundere pentru acțiunile sale sau angajamentele luate.

CertDigital furnizează servicii în concordanță cu legislația și practicile în domeniu. Cheile autorității de certificare sunt protejate folosind module hardware de securitate (Hardware Security Module - HSM), certificate conform FIPS 140-1 și FIPS 140-2 nivel 3. CertDigital implementează controalele fizice și procedurale ale sistemului.

Autoritatea de Certificare CertDigital emite certificate de diferite Clase, având nivele de credibilitate diferite. Credibilitatea certificatului depinde de procedura de verificare a identității abonatului și de efortul depus de operatorii CertDigital pentru a verifica datele trimise de către solicitant în cererea sa de înregistrare. Clasa certificatului poate, de asemenea, să depindă de Clasa de securitate a serverului sau dispozitivului de rețea pentru care se emite certificatul. Specialiștii CertDigital pot verifica starea tehnică și Clasa de securitate a sistemului informatic al unui abonat înainte de a emite un certificat din cea mai înaltă Clasă de credibilitate.

Autoritatea de Certificare CertDigital CA emite certificate pentru publicul larg și furnizează servicii specifice unei infrastructuri de chei publice. Printre cele mai importante aplicații ale certificatelor emise de CertDigital CA, se numără (fără a se limita la):

- Semnarea documentelor electronice,
- Securizarea mesajelor de e-mail (poștă electronică),
- Securizarea tranzacțiilor Web,

- Securizarea comunicațiilor de rețea,
- Semnarea codului pentru aplicații,
- Marcarea timpului.

### 2.1 Certificate de Clasă 1

Certificatele de Clasă 1 sunt emise de Autoritatea de Certificare **Cert Digital Simple CA** și **CertDigital Simple CA G2**. Aceste certificate sunt folosite numai pentru scopuri și utilizări interne și nu oferă nici o garanție asupra identității subiectului. Certificatele simple sunt destinate în principal pentru testarea performanței aplicațiilor sau dispozitivelor înainte de cumpărarea certificatelor finale. Autoritatea de **Certificare Cert Digital Simple CA** și **CertDigital Simple CA G2** emite certificate pentru aproape toate scopurile. În majoritatea cazurilor, în timpul procesului de înregistrare se verifică adresa căsuței de mesagerie electronică și/sau numele și prenumele persoanei fizice sau al reprezentantului persoanei juridice.

Certificatele de Clasa 1 conțin următorul identificator de politică:

**{CertDigital}\*id-policy(1) id-cp(1)id-Class-1(1)**

CertDigital nu își asumă nici o obligație financiară și nu oferă nici o garanție pentru certificatele (și conținutul acestora) emise în cadrul politicii de mai sus.

---

\* {CertDigital}=1.3.6.1.4.1.47898= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). CertDigital's IANNA assigned number (47898)

## 2.2 Certificate de Clasă 2

Certificatele de Clasă 2 sunt emise de Autoritățile de Certificare **Cert Digital Organization CA Class 2** și **CertDigital Organization CA Class 2 G2**. Acestea sunt certificate personale și sunt destinate în principal pentru securizarea corespondenței electronice sau autentificarea clienților în timpul sesiunilor online. Operatorii Autorităților de Certificare Cert Digital Organization CA Class 2 și CertDigital Organization CA Class 2 G2 verifică datele furnizate de clienți în timpul procesului de certificare. Identitatea persoanei fizice solicitante sau a reprezentantului persoanei juridice este supusă unei verificări detaliate. Autenticitatea adresei căsuței de mesagerie electronică inclusă în certificat este de asemenea verificată.

Certificatele de Clasa 2 conțin următorul identificator de politică:

**{CertDigital}.id-policy(1).id-cp(1).id-Class-2(2)**

Certificatele emise în cadrul acestei politici oferă garanții și responsabilități limitate.

## 2.3 Certificate de Clasă 3

Certificatele de Clasă 3 sunt emise de către 4 Autorități de Certificare: **Cert Digital Enterprise CA Class 3**, **CertDigital Enterprise CA Class 3 G2**, **Cert Digital Qualified CA Class 3**, **CertDigital Qualified CA Class 3 G2**.

Certificatele emise în această clasă pot fi certificate calificate sau certificate pentru securizarea obiectelor binare și protecția transmisiilor de date utilizând protocoalele IPsec, SSL și TLS. Operatorii CertDigital verifică datele furnizate de clienți (organizații sau instituții) în timpul procesului de înregistrare. Toate datele ce urmează a fi incluse în certificat sunt verificate.

Pe baza unui certificat emis de Cert Digital Enterprise CA Class 3, CertDigital Enterprise CA Class 3 G2, Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2 se poate determina cu exactitate identitatea unui subiect sau autenticitatea unei organizații.

CertIFICATELE calificate emise de Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2 pot fi utilizate pentru crearea de semnături electronice care să înlocuiască semnăturile olografe.

**CertIFICATELE calificate** sunt emise de Autoritățile de Certificare **Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2**. Aceste certificate sunt conforme cu Directiva 1999/93/EC a Parlamentului European referitoare la Cadrul Comunitar privind Semnatura Electronica, Legea Semnaturii Electronice 455/2001 din România și Hotărârea de Guvern 1259/Decembrie 2001 privind Normele de Aplicare ale Legii Semnaturii Electronice.

Autoritățile de certificare Cert Digital Enterprise CA Class 3 și Cert Digital Qualified CA Class 3 folosesc un certificat emis cu algoritmul sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) iar CertDigital Enterprise CA Class 3 G2, CertDigital Qualified CA Class 3 G2 folosesc un certificat emis cu algoritmul sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

CertIFICATELE de Clasa 3 conțin următorul identificator de politică:

**{CertDigital} id-policy(1) id-cp(1)id-Class-3(3)**

În plus, pentru certificatele calificate se adaugă identificatorul de politică

**itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1),**

pentru certificatele emise de **CertDigital Enterprise CA Class 3 G2** se adaugă identificatorul de politică

**{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)  
certificate-policies(1) baseline- requirements(2) subject-identity-validated(2)}  
(2.23.140.1.2.2)**

Responsabilitatea financiară a CertDigital pentru datele din certificatele emise în cadrul politicii de mai sus este prezentată în Codul de Practici și Proceduri (CPP) (a se vedea

<http://www.certdigital.ro/repository>). Certificatele emise în cadrul acestei politici oferă garanții și responsabilități complete.



## 2.4 Certificate de Clasă 4

Certificatele de Clasă 4 sunt emise de Autoritățile de Cert Digital Non-Repudiation CA Class 4 și

CertDigital NonRepudiation CA Class 4 G2. Aceste certificate sunt destinate în principal Autorităților de Certificare subordonate sau altor furnizori de servicii de încredere (OCSP sau Autorități de Marcare Temporală). Operatorii Cert Digital Non-Repudiation CA Class 4 și CertDigital NonRepudiation CA Class 4 G2 verifică identitatea clienților care trebuie să se prezinte personal la unul din ghișeele CertDigital. Se vor verifica împuternicirea din partea firmei, autenticitatea și corectitudinea documentelor de identitate furnizate precum și actele organizației. Cert Digital Non-Repudiation CA Class 4 și CertDigital NonRepudiation CA Class 4 G2 acceptă și documente autentificate de către un notar. Pe baza unui certificat emis de Cert Digital Non-Repudiation CA Class 4 și CertDigital NonRepudiation CA Class 4 G2 se poate determina cu exactitate identitatea unui subiect, autenticitatea unei organizații sau credibilitatea unei Autorități de Certificare externe. Cheile abonatului ce deține un certificat de Clasă 4 trebuie protejate utilizând module hardware de securitate (HSM).

Certificatele de Clasă 4 conțin următorul identificator de politică:

**{CertDigital} id-policy(1) id-cp(1)id-Class-4(4)**

Certificatele emise în cadrul acestei politici oferă garanții și responsabilități complete.

Abonatul CertDigital poate alege tipul de certificat potrivit nevoilor sale. Tipurile de certificate sunt descrise pe larg în Codul de Practici și Proceduri (CPP) care poate fi consultat pe site-ul Web al [CertDigital](http://CertDigital.ro). De asemenea, aceste informații pot fi primite și prin poștă electronică trimițând un mesaj la adresa: [office@certdigital.ro](mailto:office@certdigital.ro).

### 3. Jetoane de ne-repudiere

Jetoanele de ne-repudiere sunt structuri de date (mesaje) conținând cel puțin:

- informațiile furnizate de către client (de exemplu, valoare hash, numărul serial al certificatului, numărul cererii etc.) unei autorități de ne-repudiere și
- semnatura electronica a autorității respective.

Autoritățile de ne-repudiere care oferă servicii clienților sunt afiliate la CertDigital.

Prin emiterea unui jeton, o autoritate de ne-repudiere confirmă apariția unui eveniment în momentul creării acestuia sau la un moment de timp anterior. Acest eveniment poate fi: transmiterea unui document, data creării semnăturii etc.

Entitatea parteneră poate verifica, pe baza datelor recepționate, corectitudinea semnăturii bazându-se pe încrederea în CertDigital CA.

#### 3.1 Mărcile Temporale

Mărcile temporale sunt emise de catre Autoritatile Cert Digital Time Stamping Authority si CertDigital Timestamping Authority G2. Mărcile temporale, ca element de bază în asigurarea ne-repudierii, sunt emise atât persoanelor private cât și celor aparținând unei organizații. Mărcile temporale pot fi încorporate în:

- semnături electronice,
- acceptarea tranzacțiilor electronice,
- arhivarea datelor,
- notarizarea documentelor electronice etc.

Regulile ce stabilesc modul de operare al Autorității de Marcare Temporală precum și alte informații suplimentare legate de acest sistem sunt descrise într-un document separat (a se vedea Politica Generala de Marcare Temporală).

Jetonul de marcare temporală conține următorul identificator de politică:

**{CertDigital}\*.id-Time-Stamping(2).Id-Policy(1)**

---

\* {CertDigital}=1.3.6.1.4.1.47898= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). CertDigital's IANNA assigned number (47898)

Responsabilitatea financiară a CertDigital pentru timpul, data și alte informații suplimentare incluse în mărcile temporale emise în cadrul politicii de mai sus este prezentată în Politica Generala de Marcare Temporală CertDigital (a se vedea <http://www.certdigital.ro/repository> ). Cert Digital Time Stamping Authority și CertDigital Timestamping Authority G2 oferă garanții pentru mărcile temporale emise în limitele specificate în Politica generală de marcă temporală.

### **3.2 Răspunsul de confirmare OCSP**

Răspunsurile OCSP (Online Certificate Status Protocol) sunt emise de Autoritatea **CertDigital Validation Authority G2**. Răspunsurile OCSP sunt utilizate în principal pentru determinarea stării certificatelor. Aceste servicii sunt disponibile public și reprezintă o alternativă la Listele de Certificate Revocate (Certificate Revocation List – CRL). CertDigital Validation Authority G2 oferă garanții pentru răspunsurile OCSP emise, în limitele descrise în CPP. Modul de funcționare al autorității OCSP și informații suplimentare privind acest serviciu sunt prezentate pe pagina web (a se vedea <http://www.certdigital.ro>) și în CPP.

## **4. Garanțiile oferite de CertDigital**

În funcție de tipul de certificat emis, CertDigital garantează că va depune efortul necesar pentru a verifica în mod corespunzător informațiile incluse în cadrul certificatelor (a se vedea Codul de Practici și Proceduri - Capitolul 2.1.1: Obligații). Verificarea informațiilor este importantă în primul rând pentru entitățile partenere ce primesc mesaje de la un abonat care se identifică printr-un certificat digital calificat emis de CertDigital. În consecință, CertDigital este responsabilă din punct de vedere financiar pentru pagubele rezultate ca urmare a neglijenței sau erorilor comise de CertDigital în ceea ce privește aceste tipuri de certificate. Responsabilitățile CertDigital depind de clasa certificatului abonatului, iar responsabilitatea este atât față de abonat cât și față de entitățile partenere care au încredere în informațiile din certificat (a se vedea Codul de Practici și Proceduri).

Garanțiile CertDigital pot fi limitate de anumite restricții. Aceste restricții sunt aduse la cunoștință abonatului care confirmă acest lucru în cadrul unei declarații (a se vedea declarația de Acceptare a Certificatului). CertDigital garantează unicitatea semnăturilor electronice pentru abonații săi.

## **5. Acceptarea certificatului**

Responsabilitățile și garanțiile CertDigital se aplică din momentul acceptării certificatului de către abonat. Modalitatea de furnizare a certificatului și acceptanța certificatului sunt descrise în Codul de Practici și Proceduri (a se vedea capitolul 3.5 Acceptarea Certificatului) și sunt detaliate în acordurile încheiate cu abonații.

## **6. Serviciul de certificare**

CertDigital furnizează patru servicii de bază:

- I. înregistrarea,
- II. emiterea unui certificat digital,
- III. reînnoirea unui certificat,
- IV. revocarea unui certificat și
- V. verificarea stării unui certificat.

CertDigital oferă și următoarele servicii de ne-repudiere:

- VI. Autoritate de Marcare Temporală,
- VII. Serviciu de validare on-line a stării certificatelor digitale.

Înregistrarea are ca scop verificarea identității unui abonat și precedă operațiunea de emiteră a certificatului (a se vedea Codul de Practici și Proceduri, capitolul 3.1 Cererea unui certificat și Capitolul 3.2 Emiterea certificatului digital).

Reînnoirea unui certificat are loc atunci când un abonat înregistrat deja dorește să obțină un certificat pentru o aceeași cheie publică cu modificarea perioadei de valabilitate (a se vedea Codul de Practici și Proceduri, Capitolul 3.7 Prelungirea perioadei de valabilitate pentru un certificat valid).

Revocarea unui certificat are loc atunci când cheia privată corespunzătoare cheii publice din certificatul digital a fost compromisă sau este susceptibilă că ar putea fi compromisă (a se vedea Codul de Practici și Proceduri, Capitolul 3.6 Revocarea unui certificat).

Verificarea stării unui certificat este un serviciu prin care CertDigital confirmă validitatea unui certificat digital, folosind Listele de Certificate Revocate (CRL) emise de autoritățile afiliate. Verificarea stării unui certificat se poate realiza și prin intermediul serviciului de validare on-line a stării certificatelor (a se vedea Codul de Practici și Proceduri).

CertDigital permite ca fiecare pereche de chei (privată-publică) să fie generată de către abonat. CertDigital poate face recomandări cu privire la dispozitivele pentru generarea cheilor. În anumite condiții specifice, CertDigital poate genera perechi de chei unice și livra aceste chei abonaților.

## **7. Entitatea Partener**

Entitatea partener este obligată să verifice în mod corespunzător fiecare semnătură electronică de pe documentele recepționate (inclusiv certificatul digital). Pe timpul procesului de verificare, entitatea partener trebuie să utilizeze procedurile și resursele puse la dispoziție de CertDigital. Acestea specifică, printre altele, faptul că trebuie verificată lista de certificate revocate publicată de CertDigital și căile de certificare permise (a se vedea Codul de Practici și Proceduri, Capitolul 1.4.2 Autoritatea de înregistrare).

Fiecare document pentru care există probleme la verificarea semnăturii digitale trebuie să fie respins și trebuie să fie verificat prin alte modalități sau proceduri, de exemplu verificarea documentului la un notar.

## **8. Abonatul**

Abonatul este obligat să păstreze în siguranță cheia sa privată, pentru a preveni accesul neautorizat la aceasta al unei terțe părți. În cazul în care există bănuiala că a fost accesată de o terță parte, abonatul este obligat să anunțe imediat autoritatea care a emis certificatul sau digital. Informațiile furnizate autorității trebuie să fie suficiente pentru a determina cu exactitate identitatea persoanei căreia i se va revoca certificatul digital.

## **9. Actualizarea politicii de certificare**

Politica de certificare a 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 de certificare trebuie să trimită către CertDigital o declarație în acest sens și să renunțe la serviciile oferite de CertDigital.

## **10. Taxe**

Serviciile de certificare furnizate de CertDigital sunt disponibile comercial. Tarifele pentru aceste servicii depind de clasa certificatelor emise sau deținute de un abonat și de tipul de serviciu cerut. Tarifele sunt prezentate în listele de prețuri, disponibile pe site-ul CertDigital (<http://www.certdigital.ro>).