



# **Politica Serviciilor de Certificare CertDigital**

<b>EMISA DE:</b>		
<b>DEPARTAMENT</b>	<b>NUME</b>	<b>DATA</b>
COMPARTIMENT SERVICII ELECTRONICE	SEF COMPARTIMENT	19.03.2011

<b>APROBATA DE:</b>		
<b>DEPARTAMENT</b>	<b>NUME</b>	<b>DATA</b>
MANAGEMENTUL POLITICILOR SI PROCEDURILOR	MANAGER SERVICII ELECTRONICE	01.06.2016

<b>ISTORICUL MODIFICARILOR :</b>			
<b>VERSIUNE</b>	<b>AUTOR</b>	<b>DETALII MODIFICARI</b>	<b>DATA:</b>
1.0.0	SEF COMPARTIMENT	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

1.1	<b>MANAGER SERVICII ELECTRONICE</b>	Revizuire si aliniere la cerintele Regulamentului European nr. 910/2014	19.04.2017
1.2	<b>DIRECTOR TEHNIC</b>	Revizuire document	31.01.2019
1.3	<b>DIRECTOR TEHNIC</b>	Adaugare Autoritati CertDigital CA G3	30.06.2019
1.4	<b>DIRECTOR TEHNIC</b>	Revizie document	31.01.2020
1.5	<b>DIRECTOR TEHNIC</b>	Revizie document	31.01.2021
1.6	<b>MANAGER SERVICII ELECTRONICE</b>	Adaugare Autoritati CERTDIGITAL CA G4	30.06.2023

## Cuprins

1. Introducere.....	5
1.1. Marca CertDigital .....	5
1.2. Informații generale .....	5
1.3. Conținut .....	6
1.4. Servicii generale .....	8
2. Certificatele digitale.....	9
2.1 Certificatele simple (necalificate).....	11
2.2 Certificatele calificate .....	13
3. Mărcile Temporale .....	17
4. OCSP .....	18
5. Responsabilități.....	19
5.1 Responsabilitățile Furnizorului de Servicii de Certificare (FSC).....	20
5.2 Responsabilitățile utilizatorilor finali.....	21
5.3 Responsabilitățile entităților partenere .....	22
5.4 Responsabilități financiare .....	22
6. Politica de personal.....	24
7. Politica de preturi .....	26
8. Actualizarea politicii de certificare .....	27

## **1. Introducere**

### **1.1. Marca CertDigital**

CertDigital reprezintă marca înregistrată sub egida căruia S.C. Centrul de Calcul S.A. furnizează serviciile de certificare și marcarea 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. Informații generale**

Politica de certificare descrie principiile generale pe care Furnizorul de Servicii de Certificare CertDigital ("FSC") le utilizează în furnizarea serviciilor de certificare, care emite, administrează, revocă și reînnoiește certificatele în conformitate cu prevederile reglementărilor legale în materie, și anume:

- Legea nr. 455/2001 privind semnătura electronică,
- Legea nr. 451/2004 privind marca temporală,
- Hotărârea Guvernului nr. 1259/2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, cu modificările ulterioare,
- Ordinul ministrului comunicațiilor și societății informaționale nr. 492 din 15 iunie 2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală,
- Ordinul nr. 449/2017 privind aplicarea prevederilor Regulamentului (UE) nr. 910/2014.
- Standardul ETSI TS 101 456 v1.4.3 (2007-05) – "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates",
- Standardul ETSI TS 102 042 v2.1.1 (2009-05) – „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”,

- Standardul ETSI TS 102 023 v1.2.2 (2008-10) – “Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities”,
- Standardul ETSI EN 319 411– “Electronic Signatures and Infrastructures (ESI),
- Directiva 1999/93/EC a Parlamentului European și al Consiliului European și încheiată la 13 Decembrie 1999 privind stabilirea cadrului comunitar pentru semnătură electronică, cu modificările și completările ulterioare.

### 1.3. Conținut

Politica Serviciilor de Certificare CertDigital (PSC) descrie regulile și principiile generale aplicate de CertDigital în procesul de certificare a cheilor publice și folosire a autorității de marcă a timpului (TSA), precum și a altor servicii.

PSC se aplică companiei S.C. CENTRUL DE CALCUL S.A., ca Autoritate de Certificare (CA), Autoritate de Înregistrare (RA) și Autoritate de Validare a certificatelor emise (VA), precum și oricăror CA-uri, RA-uri sau VA-uri aflate în relație de subordonate sau aflate în relație contractuală cu S.C. CENTRUL DE CALCUL S.A.

CertDigital oferă certificate (simple și/sau calificate) pentru orice tip de utilizator, în limita legilor în vigoare.

**Certificatele simple (necalificate)** pot fi utilizate pentru autentificarea utilizatorului, semnătură electronică (neopozabilă în justiție) și criptare (schimbul de chei simetrice).

**Certificatele calificate** pot fi utilizate pentru autentificare, semnătură electronică extinsă (bazată pe certificat calificat – opozabilă în justiție), criptare, autentificare servere Web, semnare de cod, pentru gateway-uri VPN, toate împreună sau separat (în funcție de serviciul ales de beneficiar) ca dovadă a identității în orice tip de tranzacții electronice.

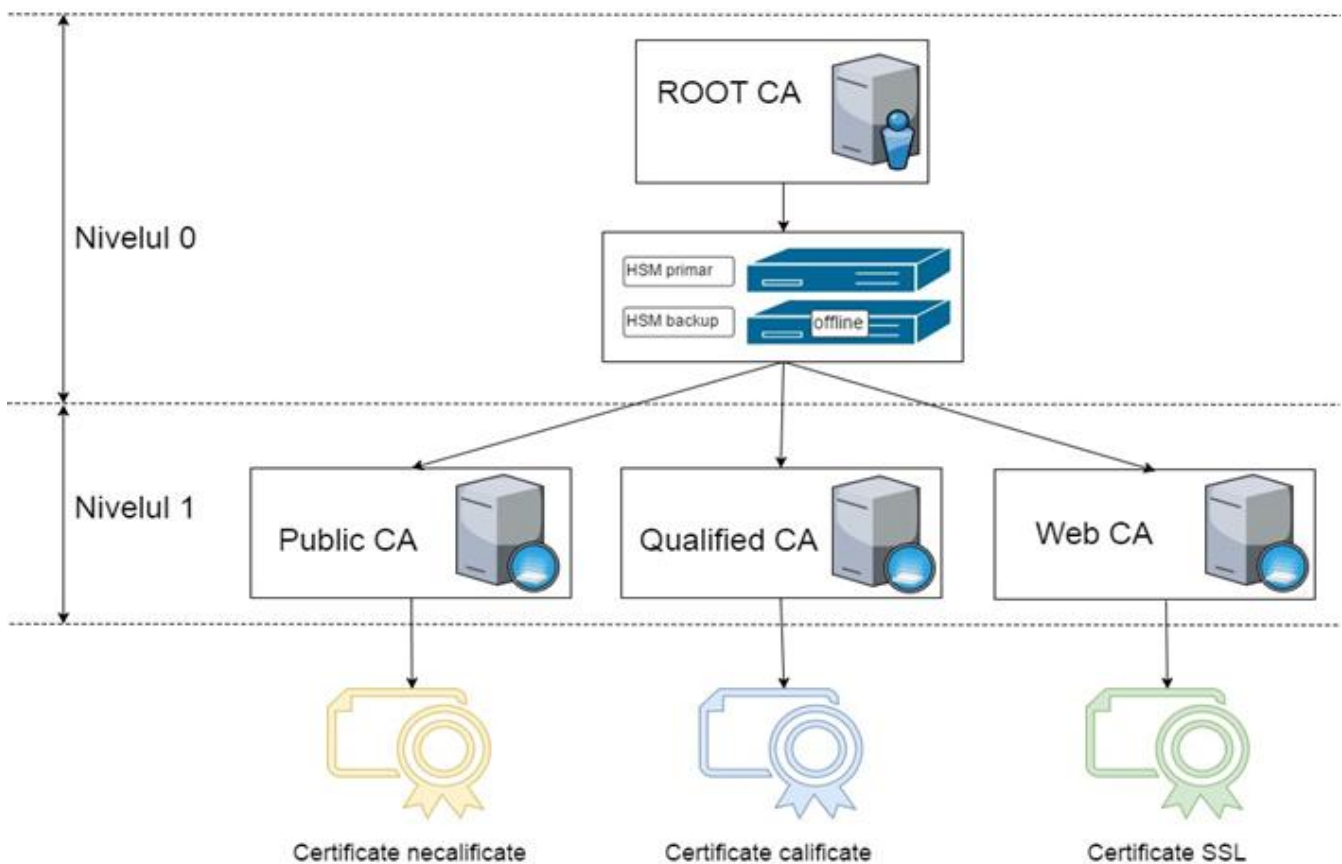
Certificatele furnizează siguranța identității utilizatorului pe baza prezentei fizice a acestuia în fața unei persoane care îi confirmă identitatea, folosind cel puțin o formă de identificare recunoscută de autorități.

Politica de Servicii 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 Declarația Practicilor Serviciilor de Certificare (DPSC) respectiv în Declarația Practicilor Serviciilor de Marcare Temporală (DPSMT).

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



Arhitectura infrastructurii de Chei Publice (PKI) a CertDigital CA

#### **1.4. Servicii generale**

Principalele clase de servicii oferite de CertDigital ca Furnizor de Servicii de Certificare sunt:

- **emiterea de certificate digitale (simple și / sau calificate)** către utilizatorii finali (ce pot fi persoane fizice, persoane juridice, servere web sau dispozitive hardware),
- **oferirea de servicii de consultanță și/sau implementare** a infrastructurilor de chei publice (PKI), precum și a unei game variate de soluții/servicii de securitate a informației.



## **2. Certificatele digitale**

Certificatele digitale CertDigital destinate utilizatorilor permit terților (entităților partenere), participanți în procesul de comunicare electronică să verifice semnăturile digitale bazate pe certificatele emise de CertDigital. 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 semnătura 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.

Supusă legilor în vigoare, o semnătură digitală sau o tranzacție interacționând cu certificatul calificat va fi valid indiferent de locul în care certificatul calificat este emis sau de locul unde semnătura digitală a fost creată sau utilizată și indiferent de locul unde CA-ul sau utilizatorul își desfășoară activitatea.

În mod implicit (serviciul uzual pus la dispoziție), certificatele calificate CertDigital au scopuri generale. Certificatele calificate pot fi folosite la nivel global. Utilizarea certificatelor calificate nu este limitată la un anumit mediu de afaceri, cum ar fi un program pilot, un sistem de servicii financiare sau un mediu de piața virtuală.

S.C. CENTRUL DE CALCUL S.A. sau ceilalți participanți nu sunt responsabili pentru monitorizarea sau impunerea vreunei restricții în aceste medii.

Cu toate acestea, anumite certificate calificate au funcții limitate. De exemplu, certificatele PCA (Autoritățile de Certificare Primare) nu pot fi utilizate pentru alte funcții decât cele de PCA. Mai mult, certificatele pentru client se supun aplicațiilor clientului și nu pot fi folosite ca certificate de server.

Certificatele de utilizator final nu pot fi utilizate decât în limita extensiilor prezente în certificat, iar acestea sunt :

- autentificare, semnare și criptare (atât pentru certificatele simple cât și pentru cele calificate)

- certificate de server, de semnare de cod, de CA – ca serviciu suplimentar, la cererea expresă a clientului (valabil doar pentru Sub CA-urile ce emit certificate calificate).

În general, certificatele pot fi utilizate doar în scopul exprimat explicit în cererea de certificat și pentru care au fost create extensiile folosite la generarea lor.

CERTDIGITAL emite șapte tipuri de bază de certificate având arii diferite de aplicabilitate. Aceste sunt:

- **certificate simple pentru autentificare, semnare și criptare** – permit semnarea emailurilor și fișierelor, sau autentificarea unui utilizator (de exemplu prin protocolul SSL);
- **certificate calificate** – permit autentificarea utilizatorului, criptarea mesajelor și semnarea documentelor cu valoare juridică;
- **certificate pentru autentificarea serverelor și schimb de chei simetrice** – sunt folosite de serviciile care operează pe baza protoacoalelor SSL/TLS/WTLS;
- **certificate pentru semnarea codului** – folosite de programatori pentru a proteja software-ul împotriva falsificării;
- **certificate pentru Autoritățile de Certificare** – folosirea lor nu este restricționată la aria definită; aria de aplicabilitate poate fi dată de extensia din certificate ce stabilește modul în care poate fi folosită cheia privată (vezi câmpul KeyUsage, Capitolul 6 din CPP), sau de rolul acesteia (de exemplu, utilizator final, Autoritate de Certificare sau altă autoritate care furnizează servicii PKI); acest tip conține de asemenea și certificatele operaționale ale Autorităților de Certificare;
- **certificate pentru confirmarea stării unui certificat** – sunt emise pentru serverele care funcționează conform protocolului OCSP și care furnizează informații despre starea certificatelor;
- **certificate pentru Autorități de Marcare Temporală** – sunt emise serverelor care, ca răspuns la cererea unui utilizator al serviciului de time stamping, emit mărci temporale prin care asociază unor date (documente,

mesaje, semnături electronice etc.) un moment de timp pe baza căruia se poate determina secvențialitatea în timp a datelor.

Certificatele emise în concordanță cu politicile de certificare CertDigital pot fi folosite în aplicații ce satisfac cel puțin următoarele condiții :

- gestionează corespunzător cheile publice și private,
- certificatele și cheile publice asociate acestora sunt folosite în concordanță cu scopul declarat al acestora, confirmat de către CertDigital,
- dispun de mecanisme interne de verificare a stării certificatelor, de creare a căilor de certificare și controlul validității (validitatea semnăturii, data expirării etc.),
- oferă utilizatorului informații corespunzătoare despre certificate și starea acestora.

## 2.1 Certificatele simple (necalificate)

Certificatele simple oferite de CertDigital au două configurații de bază: fără QSCD și cu QSCD. Certificatele simple fără QSCD pot fi folosite la serverele web (certificate SSL – pentru schimbul securizat de chei simetrice, evitând atacul de tip „man-in-the-middle” ce funcționează în cazul schemei Diffie - Hellman) sau pentru Autorități de Certificare disponibile în locația clientului, supunându-se politicii de certificare dorită de client.

**Certificatele simple fără QSCD** conțin următorul identificator de politică (în conformitate cu standardul ETSI TS 102042 V2.1.1(2009-05) și ETSI EN 319 411):

1.3.6.1.4.1.{CentrulDeCalcul}.3.1.2.2.2.1.{id-personatype} =

1.3.6.1.4.1.{CentrulDeCalcul}.4.1.1.1.{id-personatype} =

iso(1).identified- organization(3).dod(6).internet(1).private(4).enterprise(1).

{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(2).id-

qscdpresense(2).id-keygenerator(2).id-usage(1).{id-personatype}

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-persontype} = 1 pentru persoane fizice (Natural person)

{id-persontype} = 2 pentru persoane juridice (Legal person)

**CertIFICATELE SIMPLE CU QSCD** pot fi folosite pentru autentificarea utilizatorului, semnătură electronică (dar nu semnătură electronică extinsă, în înțelesul dat de Legea 455/2001) și criptare, precum și pentru semnarea de cod. Acest nivel oferă o securitate de bază pentru informații în medii cu grad scăzut sau mediu de risc (risc fără consecințe majore). Dintre acestea, menționăm accesul la informații private acolo unde probabilitatea de apariție a unui acces neautorizat nu este foarte mare. Aceste certificate pot fi folosite pentru a autentifica și controla integritatea informației care a fost semnată și pentru a asigura confidențialitatea informației, mai ales în cazul poștei electronice.

Certificatele simple cu QSCD conțin următorul identificator de politică (în conformitate cu standardul ETSI TS 102 042 V2.1.1(2009-05) și ETSI EN 319 411):

1.3.6.1.4.1.{CentrulDeCalcul}.3.1.2.1.2.1.{id-persontype} =

1.3.6.1.4.1.{CentrulDeCalcul}.4.1.1.1.{id-persontype} =

iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1).

{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(2).id-qscdpresense(1).id-keygenerator(2).id-usage(1).{id-persontype}

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-persontype} = 1 pentru persoane fizice (Natural person)

{id-persontype} = 2 pentru persoane juridice (Legal person)

## **2.2 Certificatele calificate**

Certificatul calificat reprezintă un certificat care satisface condițiile prevăzute la art. 18 din Legea 455/2001, respectiv prevederile Regulamentului (UE) nr. 910/2014 și care este eliberat de un furnizor de servicii de certificare ce satisface condițiile prevăzute la art. 20 din aceeași lege.

Aceste certificate pot fi utilizate pentru :

- autentificare, creare de semnături electronice extinse, criptare, semnare de cod – cu QSCD.
- autentificare servere Web, certificate de CA – fără QSCD.

Semnătură electronică extinsă (care este bazată doar pe un certificat calificat) reprezintă acea semnătură electronică care îndeplinește cumulativ următoarele condiții:

- a) este legată în mod unic de semnatar;
- b) asigură identificarea semnatarului;
- c) este creată prin mijloace controlate exclusiv de semnatar;
- d) este legată de datele în formă electronică, la care se raportează în așa fel încât orice modificare ulterioară a acestora este identificabilă.

Acest nivel se recomandă pentru asigurarea securității informației în medii unde există riscul apariției de breșe de securitate iar consecințele acestor breșe sunt moderate sau mari. Certificatele pot fi folosite pentru protecția tranzacțiilor financiare sau a tranzacțiilor în care există șanse de apariție a fraudelor.

Aceste certificate pot fi folosite pentru protecția tranzacțiilor de valoare nelimitată (dacă nu se specifică altceva în certificat), a tranzacțiilor în care există mari șanse de apariție a fraudelor.

**CertIFICATELE calificate cu QSCD generate de subiect** conțin următoarele identificatoare de politică (în conformitate cu standardul ETSI TS 101 456 V1.4.3 (2007-05) și ETSI EN 319 411):

- Policy Identifier = 0.4.0.194112.1.2
- 1.3.6.1.4.1.{CentrulDeCalcul}.3.1.3.1.1.1.{id-personatype} =
- 1.3.6.1.4.1.{CentrulDeCalcul}.4.1.1.1.{id-personatype} =  
iso(1).identified- organization(3).dod(6).internet(1).private(4).enterprise(1).  
{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(3).id-  
qscdpresense(1).id-keygenerator(1).id-usage(1).{id-personatype}

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-personatype} = 1 pentru persoane fizice (Natural person)

{id-personatype} = 2 pentru persoane juridice (Legal person)

**CertIFICATELE calificate cu QSCD generate de autoritate** conțin următorul identificator de politică (în conformitate cu standardul ETSI TS 101 456 V1.4.3 (2007-05) și ETSI EN 319 411):

- Policy Identifier = 0.4.0.194112.1.2
- 1.3.6.1.4.1.{CentrulDeCalcul}.3.1.3.1.2.1.{id-personatype} =
- 1.3.6.1.4.1.{CentrulDeCalcul}.4.1.1.1.{id-personatype} =  
iso(1).identified- organization(3).dod(6).internet(1).private(4).enterprise(1).  
{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(3).id-  
qscdpresense(1).id-keygenerator(2).id-usage(1).{id-personatype}

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-personstype} = 1 pentru persoane fizice (Natural person)

{id-personstype} = 2 pentru persoane juridice (Legal person)

**CertIFICATELE CALIFICATE PENTRU SIGILII ELECTRONICE CU QSCD generate de subiect** conțin următorul identificator de politică (în conformitate cu standardul ETSI TS 101 456 V1.4.3 (2007-05) și ETSI EN 319 411):

- Policy Identifier = 0.4.0.194112.1.3
- 1.3.6.1.4.1.{CentrulDeCalcul}.3.1.3.1.1.2.{id-personstype} =
- 1.3.6.1.4.1.{CentrulDeCalcul}.4.1.1.1.{id-personstype} =  
iso(1).identified- organization(3).dod(6).internet(1).private(4).enterprise(1).  
{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(3).id-  
qscdpresense(1).id-keygenerator(1).id-usage(2).{id-personstype}

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-personstype} = 2 pentru persoane juridice (Legal person)

**CertIFICATELE CALIFICATE PENTRU SIGILII ELECTRONICE CU QSCD generate de autoritate** conțin următorul identificator de politică (în conformitate cu standardul ETSI TS 101 456 V1.4.3 (2007-05) și ETSI EN 319 411) :

- Policy Identifier = 0.4.0.194112.1.3
- 1.3.6.1.4.1.{CentrulDeCalcul}.3.1.3.1.2.2.{id-personstype} =
- 1.3.6.1.4.1.{CentrulDeCalcul}.4.1.1.1.{id-personstype} =  
iso(1).identified- organization(3).dod(6).internet(1).private(4).enterprise(1).  
{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(3).id-  
qscdpresense(1).id-keygenerator(2).id-usage(2).{id-personstype}

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-persontype} = 2 pentru persoane juridice (Legal person)

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

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



### 3. Mărcile Temporale

Mărcile temporale sunt emise de către Autoritatea CertDigital Time Stamping Authority. 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 (Declaratia Practicilor Serviciilor de Marcare Temporală).

**CertIFICATELE calificate pentru mărcile** conțin următorul identificator de politică (în conformitate cu standardul ETSITS 101 456 V1.4.3(2007-05) și ETSI EN 319411):

- Policy Identifier = 0.4.0.194112.1.3
- 1.3.6.1.4.1.{CentrulDeCalcul}.3.1.3.1.2.3.2 =
- 1.3.6.1.4.1.{CentrulDeCalcul}.4.2.2.1.2 =  
iso(1).identified- organization(3).dod(6).internet(1).private(4).enterprise(1).  
{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(3).id-  
qscdpresense(1).id-keygenerator(2).id-usage(3).{id-persontype}(2)

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-usage} = 3 – Time Stamping Authority Certificate

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 Declaratia Practicilor Serviciilor de Marcare Temporală.

CertDigital Timestamping Authority oferă garanții pentru mărcile temporale emise în limitele specificate în Declarația Practicilor Serviciilor de Marcare Temporală.

#### **4. OCSP**

Răspunsurile OCSP (Online Certificate Status Protocol) sunt emise de fiecare Autoritatea de certificare și validare CertDigital.

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).

**Certificatele OCSP** conțin următorul identificator de politică (în conformitate cu standardul ETSITS 101 456 V1.4.3(2007-05) și ETSI EN 319411):

- Policy Identifier = 0.4.0.194112.1.3
- 1.3.6.1.4.1.{CentrulDeCalcul}.3.1.3.1.2.4.2 =
- 1.3.6.1.4.1.{CentrulDeCalcul}.4.2.2.1.2 =  
iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1).  
{CentrulDeCalcul}(47898).id-policy(3).id-cp(1).id-class(3).id-  
qscdpresense(1).id-keygenerator(2).id-usage(4).{id-personatype}(2)

unde :

{CentrulDeCalcul} = 47898 reprezintă numărul desemnat de IANA pentru CENTRUL DE CALCUL S.A. (poate fi consultat la adresa [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers)).

{id-usage} = 4 - OCSP Certificate

Serviciile de validare OCSP CertDigital oferă garanții pentru răspunsurile OCSP emise, în limitele descrise în CPP. Modul de funcționare al serviciului OCSP și

informații suplimentare privind acest serviciu sunt prezentate pe pagina web (a se vedea <https://www.certdigital.ro>) și în Declarația Practicilor Serviciilor de Certificare.

## **5. Responsabilități**

Răspunderea CENTRUL DE CALCUL S.A. ca furnizor de servicii de certificare este reglementată de lege în sensul că, în art. 41 din Legea nr. 455/2001 privind semnătura electronică, se prevede că furnizorul de servicii de certificare, care eliberează certificate prezentate ca fiind calificate sau care garantează asemenea certificate, este răspunzător pentru prejudiciul adus oricărei persoane care își întemeiază conduita pe efectele juridice ale respectivelor certificate :

- în ceea ce privește exactitatea, în momentul eliberării certificatului, a tuturor informațiilor pe care le conține;
- în ceea ce privește asigurarea că, în momentul eliberării certificatului, semnatarul identificat în cuprinsul acestuia deține datele de generare a semnăturii corespunzătoare datelor de verificare a semnăturii menționate în respectivul certificat;
- în ceea ce privește asigurarea că datele de generare a semnăturii corespund datelor de verificare a semnăturii, în cazul în care furnizorul de servicii de certificare le generează pe amândouă;
- în ceea ce privește revocarea certificatului, în cazurile și cu respectarea condițiilor prevăzute la art. 17 alin. (1), (2) și (3);
- în privința îndeplinirii tuturor obligațiilor prevăzute la art. 13-17 și la art. 19-22, cu excepția cazurilor în care furnizorul de servicii de certificare probează că, deși a depus diligența necesară, nu a putut împiedica producerea prejudiciului.

De asemenea, CENTRUL DE CALCUL S.A. ca furnizor de servicii de certificare poate să indice în cuprinsul unui certificat calificat restricții ale utilizării acestuia, precum și limite ale valorii operațiunilor pentru care acesta poate fi utilizat, cu condiția ca respectivele restricții să poată fi cunoscute de terți.

CENTRUL DE CALCUL S.A. ca furnizorul de servicii de certificare nu va fi răspunzătoare pentru prejudiciile rezultând din utilizarea unui certificat calificat cu

Încălcarea restricțiilor prevăzute în cuprinsul acestuia (art. 42 din Legea nr. 455/2001 privind semnătura electronică).

Garanțiile și limitele responsabilității dintre o RA și CA care asistă emiterea certificatelor pe de o parte, și utilizatorul respectiv, pe de altă parte, se supun și sunt guvernate de către acordurile dintre aceștia cu respectarea legilor în vigoare.

## **5.1 Responsabilitățile Furnizorului de Servicii de Certificare (FSC)**

Centrul de Calcul S.A ca furnizor de servicii de certificare calificată, dispune de resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfășurării activităților legate de certificarea semnăturilor electronice. În acest sens, asigurarea s-a realizat prin subscrierea unei polițe de asigurare la o societate de asigurări.

Suma asigurată este conform celei stipulate de către Ministerul Comunicațiilor și Societății Informaționale, în calitate de autoritate de reglementare și supraveghere specializată în domeniu. (art. 22 din Legea nr. 455/2001 privind semnătura electronică).

Serviciile Centrul de Calcul S.A. includ, de asemenea, o garanție pentru abonați după cum urmează:

- Nu există interpretări greșite ale entităților care aprobă cererile pentru certificat sau care emit certificatul,
- Nu există erori privind informațiile referitoare la certificat, făcute de entitățile care răspund de aprobarea cererii pentru certificat, aceleași care răspund și de emiterea certificatului,
- Certificatele utilizatorilor satisfac toate cerințele acestei Politici de Certificare, precum și Codul de Practici și Proceduri,
- Serviciile de revocare și utilizarea depozitului (sau registrului) conform cu această Politică de Certificare și Codul de Practici și Proceduri în toate aspectele importante.

Acordurile părților contractante conțin o garanție pentru părți care se bazează pe un certificat în care :

- Toate informațiile din sau încorporate într-un astfel de certificat, excepție făcând informațiile neverificate despre utilizator, sunt precise;
- În cazul certificatelor apărute în registrul CENTRUL DE CALCUL S.A., certificatul a fost emis pentru o persoană fizică sau companie și utilizatorul a acceptat certificatul în concordanță cu specificațiile prezentei Politici de Certificare și a Codului de Practici și Proceduri;
- Entitățile care aprobă cererile pentru certificat și emit certificate au respectat această Politică și Codul de Practici și Proceduri atunci când au emis certificatele.

## **5.2 Responsabilitățile utilizatorilor finali**

Serviciile CENTRUL DE CALCUL S.A. cer abonaților să garanteze că:

- Fiecare semnătura digitală creată prin utilizarea cheii private corespunzătoare cheii publice din certificat este semnătura digitală a utilizatorului și că certificatul a fost acceptat și este operațional (nu este expirat sau revocat) la momentul în care semnătura digitală a fost creată;
- Nici o persoană neautorizată nu a avut acces la cheia privată a utilizatorului;
- Toate relatările făcute de utilizator în cererea pentru certificat sunt adevărate;
- Toate informațiile furnizate de utilizator și conținute de certificat sunt adevărate;
- Certificatul este folosit exclusiv pentru scopul declarat, în concordanță cu Politica de Certificare și cu CPP;
- Utilizatorul este un utilizator final, nu un CA și nu folosește cheia privată corespunzătoare cheii publice din certificat pentru semnarea digitală a oricărui certificat (sau orice alt format de cheie publică certificată) sau lista de revocare a certificatelor, ca CA sau în altă calitate.

Titularii de certificate sunt obligați să solicite, de îndată, revocarea certificatelor, în cazul în care :

- au pierdut datele de creare a semnăturii electronice;

- au motive să creadă că datele de creare a semnăturii electronice au ajuns la cunoștința unui terț neautorizat;
- informațiile esențiale cuprinse în certificat nu mai corespund realității.

### **5.3 Responsabilitățile entităților partenere**

Entitatea partener este obligată să verifice în mod corespunzător fiecare semnătura 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 și Codul de Practici și Proceduri).

Fiecare document pentru care există probleme la verificarea semnăturii digitale trebuie să fie respins și trebuie să fie verificat prin alte modalități sau proceduri.

### **5.4 Responsabilități financiare**

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 sunt detaliate în acordurile încheiate cu abonații.

În măsura limitelor legale, S.C. CENTRUL DE CALCUL S.A. solicită abonaților să o despăgubească în unul din următoarele cazuri:

- Falsitate sau relatare greșită în cererea pentru certificate;
- Relatarea greșită a unei informații importante în cererea pentru certificat, dacă relatarea greșită sau omisiunea a fost făcută din neglijență sau cu intenția de a înșela una dintre părți;
- Neprotejarea cheii private sau neluarea măsurilor de protecție necesare prevenirii, compromiterii, pierderii, dezvăluirii, modificării sau folosirii neautorizate a cheii private a utilizatorului;

- Utilizatorul a folosit un nume (inclusiv un nume comun, nume de domeniu sau adresa de e-mail), care încalcă drepturile de proprietate intelectuală a unui terț.

CENTRUL DE CALCUL S.A. va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfășurării activității de certificare persoanelor care își întemeiază conduita pe efectele juridice ale certificatelor calificate, până la concurența echivalentului în lei al sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat este fiecare prejudiciu produs, chiar dacă se produc mai multe asemenea prejudicii ca urmare a neîndeplinirii de către furnizor a unei obligații prevăzute de lege.

## **6. Politica de personal**

CertDigital garantează că se asigură că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul unei Autorități de Certificare, Validare sau Înregistrare :

- a absolvit cel puțin liceul,
- este cetățean român,
- a semnat un contract care descrie rolul și responsabilitățile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligațiile și sarcinile asociate funcției sale,
- a fost instruit cu privire la protecția datelor personale și informațiilor confidențiale sau private,
- a semnat un contract ce conține clauze referitoare la protejarea informațiilor sensitive (din punctul de vedere al securității CertDigital) și a datelor confidențiale și private ale utilizatorilor finali,
- nu îndeplinește sarcini care pot genera conflicte de interese între Autoritatea de Certificare și Autoritatea de Înregistrare care acționează în numele acesteia.

Personalul care dorește să se numere printre persoanele de încredere din CertDigital trebuie să prezinte dovada îndeplinirii cerințelor legate de trecut, calificări și experiență, necesare pentru a îndeplini în mod competent și satisfăcător responsabilitățile postului respectiv, precum și dovada oricăror acceptări guvernamentale, dacă există, necesare pentru a îndeplini servicii de certificare în baza unor contracte guvernamentale. Verificarea informațiilor cu privire la personal se repetă la cel puțin 5 ani pentru personalul care ocupă poziții de încredere.

Înainte de începerea serviciului într-o funcție de încredere, CertDigital face verificări asupra informațiilor cu privire la personal, cuprinzând următoarele :

- Confirmarea locului de muncă anterior;
- Verificarea referințelor profesionale;
- Confirmarea celei mai înalte sau relevante instituții de învățământ urmate;
- Solicitarea cazierului judiciar;



- Solicitarea rapoartelor financiare;
- Solicitarea rapoartelor privind permisul de conducere;
- Solicitarea rapoartelor privind asistenta socială.

În măsură în care, oricare dintre cerințele impuse de această secțiune, nu poate fi satisfăcută din cauza unei interziceri sau limitări din legea locală sau din cauza altor circumstanțe, CENTRUL DE CALCUL S.A. va folosi o tehnică de investigație care este permisă de lege și care furnizează informații asemănătoare, inclusiv, dar nu limitându-se la, obținerea unei verificări a trecutului, realizată de agenția guvernamentală adecvată.

## 7. Politica de preturi

Valoarea serviciilor de certificare și categoriile de servicii pentru care sunt percepute taxe sunt publicate în lista de preturi disponibilă la adresa <https://www.certdigital.ro/>.

Serviciile oferite de CENTRUL DE CALCUL S.A. sunt stabilite după cum urmează :

- **servicii de certificare individuale** – prețul este stabilit pentru fiecare serviciu în parte, de exemplu, pentru fiecare certificat vândut sau un număr mic de certificate,
- **pachete de servicii de certificare** – prețul este stabilit pentru pachete de servicii prestate unei singure entități,
- **servicii prestate pe baza de abonament** – prețul este stabilit pentru servicii prestate lunar; valoarea sumelor plătite depinde de tipul și numărul serviciilor accesate,
- **servicii indirecte** – prețul este stabilit pentru fiecare serviciu oferit clienților săi de un partener CENTRUL DE CALCUL S.A., care își bazează activitatea pe infrastructura CertDigital; de exemplu, dacă o Autoritate de Certificare comercială este certificată de CertDigital, atunci CertDigital va percepe un preț pentru fiecare certificat emis de Autoritatea de Certificare respectivă.

Plățile se vor face în numerar, prin ordin de plata, inclusiv folosind carduri bancare pe baza de factura, conform reglementarilor legale în vigoare.

CENTRUL DE CALCUL S.A. poate presta și alte servicii contra cost, cum ar fi :

- vânzarea de dispozitive criptografice de orice tip, în funcție de nevoile utilizatorului,
- generarea cheilor pentru Autoritățile de Certificare sau utilizatori,
- testarea aplicațiilor și includerea lor în lista aplicațiilor recomandate,
- vânzarea de licențe,
- activități de proiectare, implementare și instalare,
- activități de consultanță și audit în domeniul securității informației,
- vânzarea de copii tipărite ale Codului de Practici și Proceduri, Politicii de certificare, manuale, ghiduri de utilizare etc.
- cursuri de instruire.

## **8. Actualizarea politicii de certificare**

Politica Serviciilor de Certificare 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 Certificare trebuie să trimită către CertDigital o declarație în acest sens și să renunțe la serviciile oferite de CertDigital. Amendamentele la această Politică de Certificare pot fi făcute periodic de CENTRUL DE CALCUL S.A. Ele vor avea forma unui document separat care cuprinde modificările sau actualizările prezentei Politici de Certificare.

Aceste variante vor putea fi accesate în cadrul depozitului, care este localizat la adresa : <https://www.certdigital.ro/repository>.