



Politica Serviciilor de Încredere

CertDigital

EMISA DE:

DEPARTAMENT	NUME	DATA
COMPARTIMENT SERVICII ELECTRONICE	SEF COMPARTIMENT	19.03.2011

APROBATA DE:

DEPARTAMENT	NUME	DATA
MANAGEMENTUL POLITICILOR SI PROCEDURILOR	MANAGER SERVICII ELECTRONICE	01.06.2016

ISTORICUL MODIFICARILOR :

VERSIUNE	AUTOR	DETALII MODIFICARI	DATA:
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	MANAGER SERVICII ELECTRONICE	Revizuire si aliniere la cerintele Regulamentului European nr. 910/2014	19.04.2017
1.2	DIRECTOR TEHNIC	Revizuire document	31.01.2019
1.3	DIRECTOR TEHNIC	Adaugare Autoritati CertDigital CA G3	30.06.2019
1.4	DIRECTOR TEHNIC	Revizie document	31.01.2020
1.5	DIRECTOR TEHNIC	Revizie document	31.01.2021
1.6	MANAGER SERVICII ELECTRONICE	Adaugare Autoritati CERTDIGITAL CA G4	30.06.2023
1.7	MANAGER SERVICII ELECTRONICE	Actualizare document conform modificarilor legislative.	06.10.2025

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 Încredere Certificare (TSP)	20
5.2 Responsabilitățile utilizatorilor finali.....	22
5.3 Responsabilitățile entităților partenere	22
5.4 Responsabilități financiare	23
6. Politica privind personalul de încredere.....	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 încredere pentru certificate si marcare temporala. De fiecare data când in conținutul acestui document se fac referiri la CertDigital, acele referiri implica compania Centrul de Calcul S.A.

1.2. Informații generale

Politica de certificare descrie principiile generale pe care Prestator de Servicii de Încredere CertDigital ("TSP") 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 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea.;
- Regulamentul UE nr. 910/2014 al Parlamentului European si al Consiliului privind identificarea electronica si serviciile de încredere pentru tranzacțiile electronice pe piața internă;
- Ordinul nr. 449/2017 privind aplicarea prevederilor Regulamentului (UE) nr. 910/2014.
- Standardele :
 - ISO/IEC 17065;
 - ETSI EN 319 401;
 - ETSI EN 319 411-1;
 - ETSI EN 319 411-2;
 - ETSI EN 319 412;
 - ETSI EN 319 421;
 - ETSI EN 319 422;

1.3. Conținut

Politica Serviciilor de Încredere CertDigital (PSIC) 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.

PSIC 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.

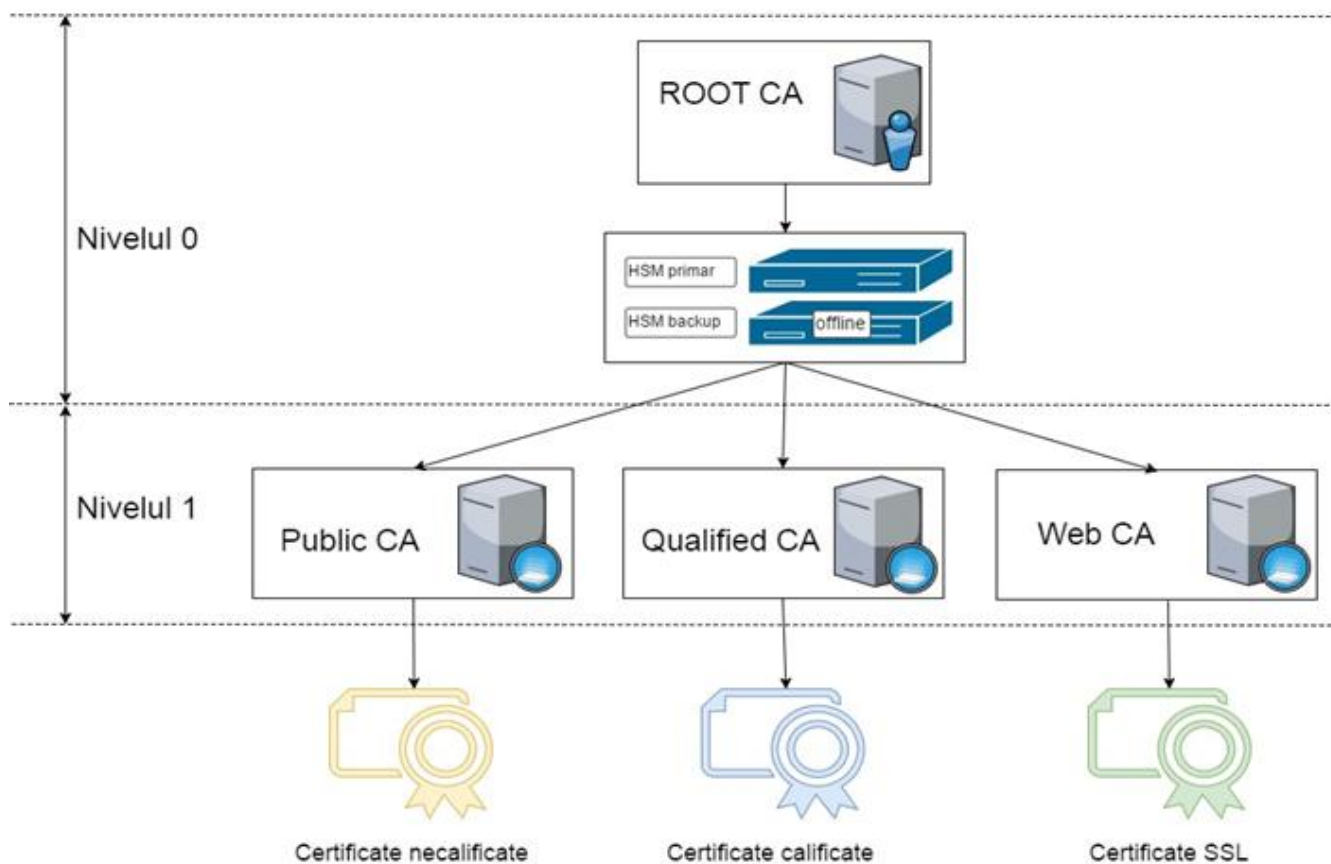
Certificatele furnizează siguranța identității utilizatorului pe baza prezentei fizice a acestuia în fața unei persoane care îi confirmă identitatea, folosind cel puțin o formă de identificare recunoscută de autorități.

Politica de Servicii de Încredere 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 Încredere pentru certificate (DPSIC) respectiv în Declarația Practicilor Serviciilor de Încredere pentru marcarea temporală (DPSIMT).

Cunoașterea Politicii Serviciilor de Încredere, precum și a Declarației Practicilor Serviciilor de Încredere 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 Prestator de Servicii de Încredere 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 protoalelor 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) si ETSI EN 319 411):

1.3.6.1.4.1.{CentrulDeCalcul}.3.1.2.2.1.{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).

{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).

{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 de: Regulamentului (UE) nr. 910/2014, Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, și care este eliberat de un furnizor de servicii de încredere.

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).

{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).

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

{id-persontype} = 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) si 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-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(3).id-
qscdpresense(1).id-keygenerator(1).id-usage(2).{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).

{id-persontype} = 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) si 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-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(3).id-
qscdpresense(1).id-keygenerator(2).id-usage(2).{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).

{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. De asemenea, aceste informații pot fi primite și prin poștă electronică trimițând un mesaj la adresa: 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,
- notarizare 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 (Declarația 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-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).

{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 Declarația 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).

{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 Încredere.

5. Responsabilități

Răspunderea CENTRUL DE CALCUL S.A., în calitate de furnizor calificat de servicii de încredere (QTSP), este reglementată de Regulamentul (UE) nr. 910/2014 (eIDAS) și de Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere. QTSP este răspunzător pentru prejudiciul adus oricărei persoane care își întemeiază conduita pe efectele juridice ale serviciilor sale calificate, în măsura în care prejudiciul rezultă din nerespectarea obligațiilor legale și a politicilor publicate (PS/CPS), cu excepția situațiilor în care QTSP dovedește că prejudiciul nu îi este imputabil.

În special, pentru certificatele calificate, QTSP răspunde:

- în ceea ce privește exactitatea, la momentul emiterii certificatului, a tuturor informațiilor pe care le conține;
- în ceea ce privește asigurarea că, la momentul emiterii certificatului, titularul identificat deține datele de generare a semnăturii corespunzătoare datelor de verificare a semnăturii menționate în respectivul certificat;
- în ceea ce privește corespondența dintre datele de generare și datele de verificare a semnăturii, în cazul în care QTSP generează sau administrează ambele (de exemplu, în cadrul serviciilor de semnătură la distanță/QSCD gestionat);
- în ceea ce privește gestionarea stării certificatului (inclusiv suspendare/revocare), potrivit cazurilor și condițiilor prevăzute de eIDAS, Legea nr. 214/2024 și politicile QTSP, astfel încât terții să poată verifica în mod rezonabil valabilitatea la momentul utilizării.

De asemenea, CENTRUL DE CALCUL S.A., ca QTSP, poate indica în cuprinsul unui certificat calificat restricții de utilizare și/sau limite valorice pentru operațiunile în care acesta poate fi folosit, cu condiția ca respectivele restricții/limite să fie ușor accesibile terților (ex.: înscrise în certificat și/sau publicate în depozitar/politici).

CENTRUL DE CALCUL S.A., ca QTSP, nu va fi răspunzătoare pentru prejudiciile rezultate din utilizarea unui certificat calificat cu încălcarea restricțiilor prevăzute în cuprinsul acestuia sau peste limitele indicate, ori fără efectuarea verificărilor rezonabile de către părțile care se bazează (inclusiv verificarea stării certificatului).

Garanțiile și limitele responsabilității dintre o RA și o CA care asistă emiterea certificatelor, pe de o parte, și utilizatorul respectiv, pe de altă parte, se stabilesc prin acordurile contractuale dintre aceștia, cu respectarea Regulamentului (UE) 910/2014, a Legii nr. 214/2024 și a politicilor publice ale QTSP (PS/CPS).

5.1 Responsabilitățile Furnizorului de Servicii de Încredere Certificare (TSP)

Centrul de Calcul S.A., în calitate de furnizor calificat de servicii de încredere (QTSP), deține resurse financiare adecvate pentru acoperirea prejudiciilor ce ar putea apărea în legătură cu activitățile de certificare a semnăturilor electronice. În acest sens, acoperirea se realizează prin poliță de asigurare încheiată la o societate de asigurări, respectând cerințele prevăzute de eIDAS, Legea nr. 214/2024 și de autoritatea de supraveghere competentă, inclusiv în ceea ce privește nivelul și condițiile minime ale garanțiilor financiare.

Suma asigurată și condițiile de acoperire sunt conforme cerințelor în vigoare stabilite de autoritatea de supraveghere pentru prestatorii calificați, în contextul procedurii de acordare, suspendare sau retragere a statutului de QTSP, reglementată prin Ordinul nr. 449/2017 (emis pentru aplicarea Regulamentului (UE) 910/2014).

Garanții față de abonați:

Serviciile Centrul de Calcul S.A. includ următoarele garanții pentru abonați:

- Nu există interpretări greșite ale entităților care aprobă cererile de certificate sau care emit certificatele.
- Nu există erori privind informațiile referitoare la certificat, imputabile entităților care aprobă cererea și emit certificatul.

- Certificatele utilizatorilor respectă cerințele politicii de certificare aplicabile și ale Declarației de Practici (CPS/PS).
- Serviciile de revocare/suspendare și funcționarea depozitarului/registrului sunt asigurate conform politicii de certificare și Declarației de Practici, în toate aspectele esențiale.

Garanții față de părțile care se bazează (relying parties)

Acordurile cu părțile contractante includ garanții pentru părțile care se bazează pe un certificat, după cum urmează:

- Toate informațiile cuprinse sau incorporate într-un astfel de certificat (cu excepția informațiilor marcate ca neverificate despre utilizator) sunt corecte la momentul emiterii.
- Pentru certificatele publicate în registrul/depozitarul CENTRUL DE CALCUL S.A., certificatul a fost emis unei persoane fizice sau unei entități juridice, iar utilizatorul a acceptat certificatul conform specificațiilor din Politica de Certificare și Declarația de Practici.
- Entitățile care aprobă cererile de certificare și emit certificate au respectat Politica și Declarația de Practici la emiterea certificatelor.
- Observații privind conformitatea și supravegherea
- Răspunderea QTSP față de abonați și terți se aplică potrivit eIDAS și Legii nr. 214/2024, în măsura în care prejudiciile rezultă din încălcarea obligațiilor legale sau a politicilor publicate, cu exonerările permise de lege (ex.: lipsa culpei QTSP, utilizare contrar restricțiilor înscrise, neefectuarea verificărilor de stare de către terți).
- Statutul de QTSP și menținerea acestuia se realizează conform Ordinului nr. 449/2017, care reglementează procedura de acordare, suspendare și retragere sub supravegherea autorității competente.
- Restricțiile de utilizare și/sau limitele valorice pot fi înscrise în certificat; QTSP nu răspunde pentru utilizări contrare restricțiilor sau peste limite, în măsura în care acestea sunt vizibile și inteligibile terților (ex.: apar în certificat și în informațiile publice ale QTSP).

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 privind personalul de încredere

CertDigital garantează că persoanele care îndeplinesc responsabilități specifice rolurilor din Autoritatea de Certificare (CA), Autoritatea de Validare sau Autoritatea de Înregistrare (RA) sunt selectate, verificate și instruite conform cerințelor legale și standardelor aplicabile.

Criterii minime pentru ocuparea funcțiilor de încredere:

- a absolvit cel puțin învățământul liceal (sau echivalent recunoscut);
- are drept de muncă în România/UE (înlocuiește cerința de „cetățean român”, care poate fi discriminatorie);
- a semnat contract individual de muncă/act de colaborare și anexă de rol (responsabilități, autorități, segregarea atribuțiilor);
- a parcurs program de formare inițială și periodică adecvat funcției (politici CA/RA/VA, securitate informațională, operațiuni, continuitate);
- a fost instruit(ă) privind protecția datelor cu caracter personal (GDPR), confidențialitatea, etica și anticorupție;
- a semnat NDA și clauze privind protejarea informațiilor sensibile (din perspectiva securității CertDigital) și a datelor confidențiale ale utilizatorilor;
- nu are conflicte de interese și respectă segregarea funcțiilor (ex.: aceeași persoană nu aprobă identitatea în RA și, simultan, emite/validează în CA pentru același caz).

Verificări la angajare și pe parcurs:

Înainte de începerea activității, CertDigital efectuează, în limitele legii și proporțional cu riscul postului:

- confirmarea identității și a dreptului de muncă;
- confirmarea angajărilor anterioare și verificarea referințelor (unde este posibil);
- confirmarea studiilor/certificărilor relevante;

- cazier judiciar sau echivalent (numai dacă este prevăzut de lege și necesar postului);
- verificări financiare (ex. incidente de fraudă/insolvență) doar pentru funcții cu risc financiar/fraudă, în baza unui temei legal și cu consimțământ informat dacă este cazul;
- permis de conducere numai pentru posturi care implică conducerea autovehiculelor în interes de serviciu.

Reverificări periodice: pentru pozițiile de încredere, cel puțin la 5 ani sau la apariția unor declanșatori (schimbare rol, incident de securitate, semnale de risc). Reverificarea este mai puțin intruzivă și ținută pe modificările apărute.

Control operațional și etic:

- Segregarea atribuțiilor și principiul „four-eyes” (dublă controlare) pentru activități critice (emitere, validare, gestionare chei).
- Principiul minimului privilegiu și control de acces bazat pe rol (RBAC), cu revizuirii periodice.
- Jurnalizare și audit al activităților relevante; trasabilitate completă.
- Obligația de declarare a conflictelor de interese și incompatibilităților, inclusiv situații sporadice.
- Offboarding controlat: retragerea imediată a accesului, returnarea echipamentelor, păstrarea NDA post-contract.

Protecția datelor și transparență:

- Prelucrările de date pentru verificări au temei legal (obligație legală, interes legitim, consimțământ – după caz), sunt minimizate și proporționale cu riscul postului.
- Candidații/angajații primesc informare transparentă (art. 13/14 GDPR): scop, temei, destinatari, retenție, drepturi.
- Retenție limitată: păstrarea datelor de screening doar pe durata necesară (ex.: durata raportului de muncă + termen legal de arhivare/audit); apoi ștergere/anonimizare.

- Acces la date strict pe bază de rol (HR/Compliance/Securitate).

Situații cu restricții legale locale:

Dacă o verificare nu poate fi efectuată din cauza unei interdicții sau limitări legale locale, CertDigital aplică o tehnică alternativă permisă (ex.: verificare efectuată de o autoritate competentă/agenție guvernamentală sau dovadă echivalentă), pentru a obține asigurări rezonabile privind integritatea și competența persoanei.

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 încredere pentru 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 încredere pentru 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 plată, inclusiv folosind carduri bancare pe baza de factură, conform reglementărilor 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>.