



Declarația de informare a PKI

EMISA DE:

DEPARTAMENT	NUME	SEMNATURA	DATA
MANAGEMENTUL POLITICILOR SI PROCEDURILOR	Ofițer de Securitate IT		30/04/2017
MANAGEMENTUL POLITICILOR SI PROCEDURILOR	Ofițer de Securitate IT		31/05/2017

LISTA DE DISTRIBUIRE :

DESTINATIA :	DATA
PUBLIC - INTERNET	31/05/2017

APROBATA DE :

DEPARTAMENT	NUME	SEMNATURA	DATA
COMITETUL DE MANAGEMENT AL POLITICILOR SI PROCEDURILOR	Director Tehnic		30/04/2017
COMITETUL DE MANAGEMENT AL POLITICILOR SI PROCEDURILOR	Director Tehnic		31/05/2017
COMITETUL DE MANAGEMENT AL POLITICILOR SI PROCEDURILOR	Director Tehnic		31/01/2019

ISTORICUL MODIFICARILOR :			
VERSIUNE	AUTOR	DETALII MODIFICARI	DATA:
1.0	Ofițer de Securitate IT	Publicare primei versiuni a documentului	30/04/2017
1.1	Ofițer de Securitate IT	Adăugare Autoritate de Certificare ROOT CA G3	31/05/2017
1.2	Director Tehnic	Revizuire anuală	31/01/2019
1.3	Director Tehnic	Revizie document	31/12/2020
1.4	Ofițer de Securitate IT	Adăugare Autorități CERTDIGITAL G4	30/06/2023
1.5	Ofițer de Securitate IT	Actualizare document în conformitate cu Legea 214/2024	06/10/2025
1.6	Director Tehnic	Actualizare document pentru serviciul CERTDIGITAL QPS (Qualified Preservation Service)	01/11/2025

Cuprins

1. Date de Contact	5
2. Tipuri de certificate, proceduri de validare și utilizare	6
3. Limite de încredere	27
4. Obligațiile clienților	27
5. Obligațiile părților de bază pentru verificarea statutului certificatului	28
6. Garanție limitată și renunțare / limitare a răspunderii	28
7. Acorduri aplicabile, declarație de practici de certificare, politică de certificare	29
8. Politica de confidențialitate	30
9. Politica de rambursare	30
10. Legea aplicabilă, reclamațiile și soluționarea litigiilor	30
11. Autorizații de certificare și licențe de depozit, mărci de încredere și audit	30

1. Date de Contact

S.C. CENTRUL DE CALCUL S.A.

Adresa sociala : STRADA TUDOR VLADIMIRESCU, NR.17, TARGU JIU, GORJ, COD
POSTAL : 210132

Nr de înregistrare la Registrul Comerțului: J18/103/1991

Cod Unic de Înregistrare: RO2163993

Web Site : www.certdigital.ro

Contact:

Telefon : (+40253) 214767

Fax : (+40253) 213409

Email: office@certdigital.ro

Vânzări :

Telefon : (+40724) 666643

E-mail : sales@certdigital.ro

Suport tehnic:

Telefon : 031-94.66

E-mail : suport@certdigital.ro

DPO :

Telefon : (+40253) 214767

Fax : (+40253) 213409

Email: dpo@centruldecacul.ro

2. Tipuri de certificate, proceduri de validare și utilizare

CERTDIGITAL emite următoarele tipuri de certificate, după cum este descris mai jos.

La nivelul ROOT CA G2, CERTDIGITAL emite următoarele tipuri de certificate:

Nivelul Root Certification Authority G2	Tip	Subtip
CertDigital Root Certification Authority G2	certificat CA	- certificat CertDigital Root CA G2 - certificat CertDigital Simple CA - certificat CertDigital Organization CA Class 2 G2 - certificat CertDigital Enterprise CA Class 3 G2 - certificat CertDigital Qualified CA Class 3 G2 - certificat CertDigital NonRepudiation CA Class 4G2
CertDigital Root Certification Authority G2	certificat OCSP	NA

La subnivelul Autorității de Certificare Root Certification Authority G2, CERTDIGITAL emite următoarele tipuri de certificate:

Nivelul Root Certification Authority G2	Tip	Subtip
CertDigital Simple CA	certificat necalificat	<i>Certificat necalificat pentru autentificare și semnare</i> - fără QSCD și cheie generate de subiect - cu QSCD și cheie generate de subiect - cu QSCD și cheia generată de CERTDIGITAL - fără QSCD și cheie generate de CERTDIGITAL <i>Certificat necalificat pentru criptare</i>

		▪ fără QSCD și cheie generate de subiect ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL ▪ fără QSCD și cheie generate de CERTDIGITAL <i>certificat OCSP</i>
CertDigital Organization CA Class 2 G2	certificat CA	<i>n/a</i>
CertDigital Qualified CA Class 3 G2	certificat calificat	<i>Certificat calificat pentru semnătura electronică</i> ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL
CertDigital Enterprise CA Class 3 G2	certificat de servere web	<i>Certificat calificat pentru autentificarea site-ului (QCW SSL)</i> <i>Certificat OV SSL</i> <i>Certificatul OCSP</i>
CertDigital NonRepudiation CA Class 4G2	Certificat calificat	<i>Certificat TimeStamping pentru server</i> <i>Certificatul OCSP</i>

La nivelul ROOT CA G3, CERTDIGITAL emite următoarele tipuri de certificate:

Nivelul ROOT CA G3	Tip	Subtip
CertDigital ROOT CA G3	certificat CA	▪ certificat CertDigital ROOT CA G3 ▪ certificat CertDigital PUBLIC CA G3 ▪ certificat CertDigital QUALIFIED CA G3 ▪ certificat CertDigital WEB CA G3
CertDigital ROOT CA G3	certificat OCSP	▪ NA

La subnivelul Autorității de Certificare ROOT CA G3, CERTDIGITAL emite următoarele tipuri de certificate:

Nivelul ROOT CA G3	Tip	Subtip
CertDigital PUBLIC CA G3	certificat necalificat	<i>Certificat necalificat pentru autentificare și semnare</i> ▪ fără QSCD și cheie generate de subiect ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL ▪ fără QSCD și cheie generate de CERTDIGITAL <i>Certificat necalificat pentru criptare</i> ▪ fără QSCD și cheie generate de subiect ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL ▪ fără QSCD și cheie generate de CERTDIGITAL <i>Certificat necalificat pentru sigiliu</i>

		<i>electronic</i> ▪ Fără QSCD și cheia generată de subiect ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL ▪ fără QSCD și cheie generate de CERTDIGITAL <i>certificat OCSP</i>
CertDigital QUALIFIED CA G3	certificat calificat	<i>Certificat calificat pentru semnătura electronică</i> ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL <i>Certificat calificat pentru sigiliu electronic</i> ▪ cu QSCD și cheie generate de subiect ▪ cu QSCD și cheia generată de CERTDIGITAL <i>Certificat TimeStamping pentru server</i> <i>Certificat OCSP</i>
CertDigital WEB CA G3	certificat de servere web	<i>Certificat calificat pentru autentificarea site-ului (QCW SSL)</i> <i>Certificat OV SSL</i> <i>Certificat OCSP</i>

La nivelul ROOT CA G4, CERTDIGITAL emite următoarele tipuri de certificate:

Nivelul ROOT CA G4	Tip	Subtip
CERTDIGITAL ROOT CA G4	certificat CA	- certificat CERTDIGITAL ROOT CA G4 - certificat CERTDIGITAL QUALIFIED CA G4

La subnivelul Autorității de Certificare ROOT CA G4, CERTDIGITAL emite următoarele tipuri de certificate:

Nivelul ROOT CA G4	Tip	Subtip
CERTDIGITAL QUALIFIED CA G4	certificat calificat	<i>Certificat calificat pentru semnătura electronică</i> - cu QSCD și cheie generate de subiect - cu QSCD și cheia generată de CERTDIGITAL <i>Certificat calificat pentru sigiliu electronic</i> - cu QSCD și cheie generate de subiect - cu QSCD și cheia generată de CERTDIGITAL
	certificat calificat	<i>Certificat Time Stamping pentru server</i>
	certificat calificat	<i>Certificat pentru semnare OCSP</i>
	certificat calificat	<i>Certificat pentru păstrare pe termen lung a semnăturilor electronice și a sigiliilor electronice calificate QPS.</i>

CERTDIGITAL se va asigura că elementele de identificare a subiecților și corectitudinea numelor lor și a datelor asociate sunt examinate în mod corespunzător ca parte a serviciului definit sau, după caz, încheiate prin examinarea atestărilor din surse adecvate și autorizate, conform tabelului următor :

I. La subnivelul CertDigital Root Certification Authority G2

Tipul / subtipul certificatului	Folosire	Politica de certificare	Procedura de validare
Certificat calificat pentru semnătura electronică	Numai pentru semnătura electronica	<i>Cu QSCD și cheie generate de Subiect</i> <i>CertDigital Qualified CA Class 3 G2 CPS OID :</i> <i>1.3.6.1.4.1.47898.1.1.3</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Persoana fizica se obliga sa prezinte la cererea autorității de înregistrare următoarele documente: - Acordul abonatului - Documente de identitate (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) care confirmă identitatea subiectului, Și dacă Subiectul sau Abonatul dorește să includă datele unei instituții (entitate juridică) pentru care lucrează: - Documente oficiale care demonstrează că persoana juridică acționează ca angajator al persoanei fizice sau că există un acord obligatoriu din punct de vedere juridic între ele - Declarația Identificarea trebuie făcută față în față, notar public sau prin utilizarea unui certificat calificat emis numai de CERTDIGITAL.
		<i>Cu QSCD și cheie generate de CertDigital</i> <i>CertDigital Qualified CA Class 3 G2 CPS OID :</i> <i>1.3.6.1.4.1.47898.1.1.3</i> Această politică este conformă cu standardul ETSI EN 319 411-2	

Declarația de informare a PKI

Certificat de server TimeStamping	Doar pentru semnarea Token-urilor Timestamps	<i>CertDigital NonRepudiation CA Class 4 G2 CPS OID : 1.3.6.1.4.1.47898.1.1.4</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Consultați certificatul calificat pentru semnătura electronică
Certificat OCSP	Numai pentru semnarea răspunsurilor OCSP	<i>CertDigital Qualified CA Class 3 G2 CPS OID : 1.3.6.1.4.1.47898.1.1.3</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Consultați certificatul calificat pentru semnătura electronică
Certificat server web OV SSL	Numai pentru autentificarea serverului Web	<i>CertDigital Enterprise CA Class 3 G2 CPS pentru OV SSL OID : 1.3.6.1.4.1.47898.1.1.3</i> Această politică este conformă cu standardul ETSI EN 319 411-1 și CAB Forum Cerințe de bază	Documentele de identitate (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) sunt necesare pentru identificarea persoanei fizice: - Când persoana fizică este Subiectul unui certificat digital emis de CertDigital. - Când persoana fizică reprezintă o entitate juridică care încheie un acord contractual cu CertDigital. Toate documentele sunt documente originale sau sunt certificate de un notar public. Autentificarea identității unei persoane juridice se efectuează fie prin participarea personală a reprezentantului autorizat al persoanei juridice la Autoritatea de Înregistrare sau prin participarea personală a reprezentantului autorizat al Autorității de Înregistrare la sediul entității juridice (menționat în cerere). Organizațiile românești sunt autentificate

			pe baza unor documente și atestări recente, valabile în România, organizații din alte țări ale UE, sunt autentificate pe baza documentelor și atestatele echivalente aplicabile țării în cauză. Reprezentanții autorizați ai instituției sunt obligați să prezinte la cererea Autorității de Înregistrare următoarele documente: - copie certificată "în conformitate cu originalul" certificatului de înregistrare al companiei; - Copie a facturii de utilitate (telefon, altele) emisă companiei; - Documente care atestă identitatea solicitantului (cartea de identitate sau pașaportul cetățenilor români și pașaportul cetățenilor străini) și autorizația care atestă că este reprezentantul companiei; - Cererea de achiziție; - Declarație de șablon a titularului domeniului Procedura efectuată pentru a verifica identitatea persoanei juridice și identitatea reprezentantului autorizat constă în: - Verificarea autorizației și identității reprezentantului persoanei juridice care depune cererea în numele acestei entități. - Verificarea faptului că domeniul menționat în certificat este înregistrat de entitatea care transmite cererea de certificat sau de cea care a autorizat utilizarea domeniului de către entitatea care a trimis solicitarea. Acest lucru se face folosind serviciul de identificare oferit de ROTLD la www.rotld.ro - Verificarea în serviciul de identificare operat de ICANN.
--	--	--	--

			- (www.iana.org/whois) Dacă proprietarul domeniului este cel care solicită certificatul SSL sau cel care a autorizat utilizarea domeniului solicitantului. - Verificarea în registrul regional de domenii Internet (baza de date RIPE pentru abonații europeni) dacă persoana care solicită certificatul SSL este proprietarul sau are dreptul de a utiliza adresa IP rutabilă pentru care se solicită certificatul. - Verificarea existenței, a denumirii și a adresei companiei, prin chemarea unei părți de încredere
Certificat calificat pentru certificatul de autentificare pe site (QCW SSL)	Numai pentru autentificarea serverului Web	CertDigital Organization CA Class 2 G2 CPS pentru certificate de server calificat Web (EV SSL) OID: 1.3.6.1.4.1.47898.1.1.2 Această politică este conformă cu standardul ETSI EN 319 411-2 și CA / B Forum EV Guidelines	În conformitate cu CA / B Forum Ghidul EV (www.cabforum.org), secțiunea 11. Cerințe de verificare

II. La subnivelul CertDigital ROOT CA G3

Tipul / subtipul certificatului	Folosire	Politica de certificare	Procedura de validare
Certificat calificat pentru semnătura electronică	numai pentru semnătura electronică	<i>Cu QSCD și cheie generate de Subiect</i> CertDigital QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.3.1.3.1.1.1</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Persoana fizică se obliga sa prezinte la cererea autorității de înregistrare următoarele documente: - Acordul abonatului - Documente de identitate (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) care confirmă identitatea subiectului, Și dacă Subiectul sau Abonatul dorește să includă datele unei instituții (entitate juridică) pentru care lucrează: - Documente oficiale care demonstrează că persoana juridică acționează ca angajator al persoanei fizice sau că există un acord obligatoriu din punct de vedere juridic între ele - Declarația Identificarea trebuie făcută față în față, notar public sau prin utilizarea unui certificat calificat emis numai de CERTDIGITAL.
		<i>Cu QSCD și cheie generate de CertDigital</i> CertDigital QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.3.1.3.1.2.1</i> Această politică este conformă cu standardul ETSI EN 319 411-2	

Declarația de informare a PKI

Certificat calificat pentru sigiliu electronic	numai pentru sigiliul electronic	<i>Cu QSCD și cheie generate de Subiect</i> CertDigital QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.3.1.3.1.1.2</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Reprezentanții autorizați ai instituției sunt obligați să prezinte la cererea Autorității de Înregistrare următoarele documente: - Acordul abonatului și Declarația - Extras valid din registrul comerțului (sau echivalentul străin pentru societățile străine înregistrate conform legislației străine); - Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este administratorul legal al entității - Documente care să ateste identitatea subiectului (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini); - Identificarea trebuie făcută față în față, notar public sau prin utilizarea unui certificat calificat emis numai de CERTDIGITAL.
		<i>Cu QSCD și cheie generate de CertDigital</i> CertDigital QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.3.1.3.1.2.2</i> Această politică este conformă cu standardul ETSI EN 319 411-2	
Certificat de server TimeStamping	doar pentru semnarea Token-urilor si a Timestamps.	CertDigital QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.3.1.3.1.2.3.2</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Consultați certificatul calificat pentru sigiliul electronic
Certificat OCSP	Numai pentru semnarea răspunsurilor OCSP	CertDigital QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.3.1.3.1.2.4.2</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Consultați certificatul calificat pentru sigiliul electronic.

Declarația de informare a PKI

Certificat necalificat pentru autentificare și semnare	doar pentru semnătură și autentificare electronică	<i>Cu QSCD și cheie generate După subiect</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.1.1.1.{id- persontype} Această politică este conformă cu standardul ETSI EN 319 411-1	Persoana fizica se obliga sa prezinte la cererea autorității de înregistrare următoarele documente: - Acordul abonatului - Copii ale documentelor de identitate (buletin de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) care confirmă identitatea subiectului, și dacă Subiectul sau Abonatul dorește să includă datele unei instituții (entitate juridică) pentru care lucrează - Copii ale documentelor oficiale care demonstrează că persoana juridică acționează ca angajator al persoanei fizice sau că există un acord obligatoriu din punct de vedere juridic între aceștia - Declarația Nu este necesară identificarea față-în-față.
		<i>Cu QSCD și cheie generate De către CertDigital</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.1.2.1.{id- persontype} Această politică este conformă cu standardul ETSI EN 319 411-1	
		<i>Fără QSCD și cheie Generate de subiect</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.2.1.1.{id- persontype} Această politică este conformă cu standardul ETSI EN 319 411-1	
		<i>Fără QSCD și cheie Generate de CertDigital</i> CertDigital PUBLIC CA G3 CPS	

Declarația de informare a PKI

		OID: 1.3.6.1.4.1.47898.3.1.2.2.2.1.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	
Certificat necalificat pentru sigilare	numai pentru sigilare	<i>Cu QSCD și cheie generate De către CertDigital</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.1.2.2.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	Reprezentanții autorizați ai instituției sunt obligați să prezinte la cererea Autorității de Înregistrare următoarele documente: - Acordul abonatului și Declarația - Copie a extrasului valabil al registrului comerțului (sau echivalentul străin al societăților străine înregistrate conform legislației străine); - Copie a mandatului oficial, atunci când persoana fizică care reprezintă persoana juridică nu este administratorul legal al entității - Copii de documente pentru atestarea identității subiectului (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini); Nu este necesară identificarea față-în-față.
		<i>Cu QSCD și cheie generate După subiect</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.1.1.2.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	
		Fără QSCD și cheie Generate de CertDigital CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.2.2.2.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	

Declarația de informare a PKI

		<i>Fără QSCD și cheie Generate de subiect</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.2.1.2.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	
Certificat necalificat pentru criptare	doar pentru criptare	<i>Cu QSCD și cheie generate de către CertDigital</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.1.2.5.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	Consultați certificatul necalificat pentru autentificare și semnare.
		<i>Cu QSCD și cheie generate după subiect</i> CertDigital PUBLIC CA G3 CPS OID : 1.3.6.1.4.1.47898.3.1.2.1.1.5.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-1	
		<i>Fără QSCD și cheie generate de CertDigital</i> CertDigital PUBLIC CA G3 CPS	

Declarația de informare a PKI

		OID: <i>1.3.6.1.4.1.47898.3.1.2.2.5.{id-personatype}</i> Această politică este conformă cu standardul ETSI EN 319 411-1 <i>Fără QSCD și cheie generate de subiect</i> CertDigital PUBLIC CA G3 CPS OID : <i>1.3.6.1.4.1.47898.3.1.2.2.1.5.{id-personatype}</i> Această politică este conformă cu standardul ETSI EN 319 411-1	
Certificat OCSP	doar pentru semnarea răspunsurilor OCSP	CertDigital Public CA G3 CPS OID : <i>1.3.6.1.4.1.47898.3.1.2.1.2.4.2</i> Această politică este conformă cu standardul ETSI EN 319 411-1	Consultați certificatul necalificat pentru sigiliul electronic.
Certificat server web OV SSL	numai pentru autentificarea serverului Web	CertDigital WEB CA G3 CPS pentru OV SSL OID : <i>1.3.6.1.4.1.47898.3.1.4.1.6.{id-personatype}</i> Această politică este conformă cu standardul ETSI EN 319 411-1 și Cerințele de bază a CAB Forum.	Documentele de identitate (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) sunt necesare pentru identificarea persoanei fizice: - Când persoana fizică este Subiectul unui certificat digital emis de CertDigital. - Când persoana fizică reprezintă o entitate juridică care încheie un acord contractual cu CertDigital. Toate documentele sunt documente originale sau sunt certificate de un notar public. Autentificarea identității unei persoane juridice se efectuează fie prin participarea personală a reprezentantului autorizat al persoanei juridice la Autoritatea de Înregistrare sau prin participarea personală a reprezentantului autorizat al Autorității de Înregistrare la sediul entității juridice (menționat în

			cerere). Organizațiile românești sunt autentificate pe baza unor documente și atestări recente, valabile în România, organizații din alte țări ale UE, sunt autentificate pe baza documentelor și atestatele echivalente aplicabile țării în cauză. Reprezentanții autorizați ai instituției sunt obligați să prezinte la cererea Autorității de Înregistrare următoarele documente: - copie certificată "în conformitate cu originalul" certificatului de înregistrare al companiei; - Copie a facturii de utilitate (telefon, altele) emisă companiei; - Documente care atestă identitatea solicitantului (cartea de identitate sau pașaportul cetățenilor români și pașaportul cetățenilor străini) și autorizația care atestă că este reprezentantul companiei; - Cererea de achiziție; - Declarație de șablon a titularului domeniului Procedura efectuată pentru a verifica identitatea persoanei juridice și identitatea reprezentantului autorizat constă în: - Verificarea autorizației și identității reprezentantului persoanei juridice care depune cererea în numele acestei entități. - Verificarea faptului că domeniul menționat în certificat este înregistrat de entitatea care transmite cererea de certificat sau de cea care a autorizat utilizarea domeniului de către entitatea care a trimis solicitarea. Acest lucru se face folosind serviciul de identificare oferit de ROTLD la www.rotld.ro - Verificarea în serviciul de identificare operat de ICANN. - (www.iana.org/whois) Dacă proprietarul domeniului este cel care solicită certificatul SSL sau cel care a autorizat utilizarea domeniului solicitantului. - Verificarea în registrul regional de domenii Internet (baza de date RIPE pentru abonații europeni) dacă persoana care solicită certificatul SSL este proprietarul sau are dreptul de a utiliza adresa IP rutabilă pentru care se solicită certificatul. Verificarea existenței, a denumirii și a adresei companiei, prin chemarea unei
--	--	--	--

Declarația de informare a PKI

			părți de încredere
Certificat calificat pentru certificatul de autentificare pe site (QCW SSL)	numai pentru autentificarea serverului Web	CertDigital WEB G3 CPS pentru certificate de server calificat Web (EV SSL) OID : 1.3.6.1.4.1.47898.3.1.4.1.7.{id-personatype} Această politică este conformă cu standardul ETSI EN 319 411-2 și CA / B Forum EV Guidelines	În conformitate cu CA / B Forum Ghidul EV (www.cabforum.org), secțiunea 11. Cerințe de verificare
Certificat OCSP	doar pentru semnarea răspunsurilor OCSP	CertDigital WEB CA G3 CPS pentru OV SSL OID : 1.3.6.1.4.1.47898.3.1.4.1.2.4.2 Această politică este conformă cu standardul ETSI EN 319 411-1 și Cerințe de bază din forumul CAB.	Consultați certificatul Web Server OV SSL.
<i>{id-personatype} : 1 – Natural person ; 2 – Legal person</i>			

III. La subnivelul CERTDIGITAL ROOT CA G4

Tipul / subtipul certificatului	Folosire	Politica de certificare	Procedura de validare
Certificat calificat pentru semnătura electronică	numai pentru semnătura electronica	<i>Cu QSCD și cheie generate de Subiect</i> CERTDIGITAL QUALIFIED CA G4 CPS <i>OID : 1.3.6.1.4.1.47898.4.1.1.1</i> Această politică este conformă cu standardul ETSI EN 319 411-2	Persoana fizica se obliga sa prezinte la cererea autorității de înregistrare următoarele documente: - Acordul abonatului - Documente de identitate (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) care confirmă identitatea subiectului, Și dacă Subiectul sau Abonatul dorește să includă datele unei instituții (entitate juridică) pentru care lucrează: - Documente oficiale care demonstrează că persoana juridică acționează ca angajator al persoanei fizice sau că există un acord obligatoriu din punct de vedere juridic între ele - Declarația Identificarea trebuie făcută față în față, notar public sau prin utilizarea unui certificat calificat emis numai de CERTDIGITAL.
		<i>Cu QSCD și cheie generate de CertDigital</i> CERTDIGITAL QUALIFIED CA G4 CPS <i>OID : 1.3.6.1.4.1.47898.4.2.1.1.1</i> Această politică este conformă cu standardul ETSI EN 319 411-2	

Declarația de informare a PKI

Certificat calificat pentru sigiliu electronic	numai pentru sigiliul electronic	<i>Cu QSCD și cheie generate de Subiect</i> CERTDIGITAL QUALIFIED CA G4 CPS <i>OID : 1.3.6.1.4.1.47898.4.1.1.1.2</i> Această politică este conformă cu standardul ETSI EN 319 411-1 si 319 411-2	Reprezentanții autorizați ai instituției sunt obligați să prezinte la cererea Autorității de Înregistrare următoarele documente: - Acordul abonatului și Declarația - Extras valid din registrul comerțului (sau echivalentul străin pentru societățile străine înregistrate conform legislației străine); - Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este administratorul legal al entității - Documente care să ateste identitatea subiectului (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini); - Identificarea trebuie făcută față în față, notar public sau prin utilizarea unui certificat calificat emis numai de CERTDIGITAL.
		<i>Cu QSCD și cheie generate de CertDigital</i> CERTDIGITAL QUALIFIED CA G3 CPS <i>OID : 1.3.6.1.4.1.47898.4.2.1.1.2</i> Această politică este conformă cu standardul ETSI EN 319 411-1 si 319 411-2	
Certificat de server Time Stamping	doar pentru semnarea Token-urilor si a Timestamps.	CERTDIGITAL QUALIFIED CA G4 CPS <i>OID : 1.3.6.1.4.1.47898.4.2.2.1.2</i> <i>CP : 0.4.0.194112.1.3</i> <i>Time Stamping (1.3.6.1.5.5.7.3.8)</i> Această politică este conformă cu standardul ETSI EN 319 411-1 si 319 411-2	Consultați certificatul calificat pentru TSA.

Declarația de informare a PKI

Certificat OCSP	Numai pentru semnarea răspunsurilor OCSP	CERTDIGITAL QUALIFIED CA G4 CPS <i>OID : 1.3.6.1.4.1.47898.4.2.2.1.2</i> <i>CP : 0.4.0.194112.1.3</i> <i>OCSP Signing (1.3.6.1.5.5.7.3.9)</i> Această politică este conformă cu standardul ETSI EN 319 411-1 și 319 411-2	Consultați certificatul calificat pentru OCSP.
Certificat pentru validarea semnăturilor electronice	doar pentru validarea semnăturii	CERTDIGITAL VALIDATION AUTHORITY G4 <i>OID : 1.3.6.1.4.1.47898.4.2.2.1.2</i> <i>CP : 0.4.0.194112.1.3</i> <i>Document Signing (1.3.6.1.4.1.311.10.3.12)</i> <i>Secure Email (1.3.6.1.5.5.7.3.4)</i> Această politică este conformă cu standardul ETSI EN 319 411-1, 319 411-2 și Cerințe de bază din forumul CAB.	Consultați certificatul calificat pentru validarea semnăturilor electronice.
Certificat pentru pastrarea pe termen lung semnăturilor electronice și a	Doar pentru CERTDIGITAL QPS	CERTDIGITAL Qualified Preservation Service G4 <i>OID : 1.3.6.1.4.1.47898.4.2.2.1.2</i> <i>CP : 0.4.0.194112.1.3</i> <i>Document Signing</i>	Consultați certificatul calificat pentru QPS.

Referința: 8/2017
Versiune: 1.6
Data: 01/11/2025

Declarația de informare a PKI



Pagina: 26

sigiliilor calificate		(1.3.6.1.4.1.311.10.3.12) <i>Client Authentication (1.3.6.1.5.5.7.3.2)</i> <i>Secure Email (1.3.6.1.5.5.7.3.4)</i> Această politică este conformă cu standardul ETSI EN 119 511, 119 512 și Cerințe de bază din forumul CAB.	
<i>{id-persontype} : 1 – Natural person ; 2 – Legal person</i>			

3. Limite de încredere

CERTDIGITAL va acoperi daunele pe care le-ar putea provoca din cauza serviciilor de certificare pentru persoanele care își construiesc moralitatea cu privire la efectele juridice ale certificatelor calificate până la echivalentul în lei a sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat reprezintă toate daunele cauzate chiar dacă există mai multe astfel de daune după ce furnizorul nu și-a îndeplinit obligațiile prevăzute de lege.

CERTDIGITAL va acoperi daunele pe care le-ar putea provoca datorită serviciilor de certificare pentru persoanele care își construiesc moralitatea cu privire la efectele juridice ale Certificatelor calificate pentru certificate de autentificare (QCW SSL), conform cerințelor CA / B Forum.

4. Obligațiile clienților

Clienții se angajează să:

- Respectarea regulilor acordului încheiat cu CERTDIGITAL;
- Utilizați doar perechile de chei pentru scopurile definite în Secțiunea 2 de mai sus și în conformitate cu orice alte limitări care pot fi notificate clientului;
- depunerea sau prezentarea documentelor necesare care confirmă informațiile incluse într-o cerere de certificare;
- Să aveți grijă deosebită pentru a evita utilizarea neautorizată a cheii private a subiectului.
- Notificați CERTDIGITAL, fără întârzieri nejustificate, dacă oricare dintre situațiile următoare are loc până la sfârșitul perioadei de valabilitate indicate în Certificat :
 - o cheia privată a subiectului a fost pierdută, furată sau compromisă.
 - o controlul asupra cheii private a subiectului a fost pierdut din cauza compromiterii potențiale sau reale a datelor de activare (de exemplu codul PIN) sau din alte motive.
 - o Inexactitatea sau modificarea conținutului certificatului, astfel cum a fost notificat clientului.
- Asigurați-vă că, dacă Clientul sau Subiectul generează perechea de chei a subiectului, numai Subiectul deține cheia privată.

- Aplicați certificatul și cheia privată corespunzătoare numai în scopul menționat în certificat și în conformitate cu scopurile și restricțiile enunțate în acest document.

5. Obligațiile părților de bază pentru verificarea statutului certificatului

Părțile implicate trebuie să utilizeze toate resursele pe care CertDigital le pune la dispoziție prin depozitul său pentru a verifica starea unui certificat în orice moment înainte de a se baza pe acesta. CertDigital actualizează OCSP, CRL în consecință;

6. Garanție limitată și renunțare / limitare a răspunderii

În limita stabilită de legea română, în nici un caz (cu excepția fraudei sau abaterilor intenționate), CERTDIGITAL va fi răspunzător pentru:

- Orice pierdere a profitului;
- Orice pierdere de date;
- orice daune indirecte, consecvente sau punitive rezultate din sau în legătură cu utilizarea, livrarea, licența și performanța sau neexecutarea certificatelor sau semnăturilor digitale;
- Orice alte daune.

7. Acorduri aplicabile, declarație de practici de certificare, politică de certificare

CERTDIGITAL publică în depozit <https://www.certdigital.ro/repository> următoarele documente:

- Pentru CertDigital ROOT CA G2 :
 - Declarație de practici de certificare a CertDigital Root Certification Authority G2
 - Declarație de practici de certificare a CertDigital Qualified CA Class 3 G2

- Pentru CertDigital ROOT CA G3 :
 - Declarație de practici de certificare a CertDigital ROOT CA G3
 - Declarație de practici de certificare a CertDigital QUALIFIED CA G3
 - Declarație de practici de certificare a CertDigital PUBLIC CA G3
 - Declarație de practici de certificare a CertDigital WEB CA G3 pentru certificate OV SSL
 - Declarație de practici de certificare a CertDigital WEB CA G3 pentru certificatele calificate pentru autentificarea site-ului (EV SSL).

- Pentru CertDigital ROOT CA G4 :
 - Declarație de practici de certificare a CERTDIGITAL ROOT CA G4
 - Declarație de practici de certificare a CERTDIGITAL QUALIFIED CA G4

8. Politica de confidențialitate

Toate informațiile furnizate de CERTDIGITAL au fost colectate, stocate și procesate în conformitate cu Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR, cu Legea nr. 506/2004 (actualizată) privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice

Relațiile dintre un subiect, un abonat, o parte investită și CERTDIGITAL se bazează pe încredere:

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

9. Politica de rambursare

Politica de rambursare este definită în cadrul politicii interne de prețuri. Dacă un abonat sau o parte care se bazează nu este mulțumit de servicii, aceștia pot solicita revocarea certificatelor și rambursarea taxelor numai dacă CERTDIGITAL nu își îndeplinește obligațiile și îndatoririle specificate în contractul de abonat și în prezentul document și în conformitate cu legea română.

10. Legea aplicabilă, reclamațiile și soluționarea litigiilor

Legile române vor reglementa executarea, construirea, interpretarea și validitatea prezentului document (fără a aduce atingere oricărei prevederi privind conflictul de legi care ar determina aplicarea altor legi).

11. Autorizații de certificare și licențe de depozit, mărci de încredere și audit

CA emite certificate utilizând produsele interne dezvoltate de CERTDIGITAL care au fost acreditate de NATO (NIAPC) și de către Agenția Națională de Securitate Națională (ORNISS) ca fiind capabile să protejeze informațiile CLASSIFIED.

În furnizarea de servicii de încredere, CERTDIGITAL menține mai multe acreditări și certificări.

Acestea includ:

- Webtrust pentru autorități de certificare - realizată anual de LL-C(Certification), această certificare asigură părților potențial de bază că un practician calificat a evaluat practicile și controlul de afaceri al Autorității de Certificare pentru a determina dacă sunt conforme cu Principiile și Criteriile AICPA, și a emis un raport cu o opinie fără rezerve indicând faptul că aceste principii sunt respectate.
- ISO / IEC 20000-1, care certifică faptul că Sistemul de Management al Serviciilor de Tehnologie Informației, operat de CERTDIGITAL, este în conformitate cu acest standard, pentru furnizarea următoarelor servicii: dezvoltare și întreținere pentru software și sisteme informatice; Securitatea cibernetică (de exemplu, răspunsul și analiza incidentului, evaluarea vulnerabilității și testarea penetrării, Advanced Threat Intelligence & Correlation);
- ISO 9001 care demonstrează implementarea unui sistem de management al calității, care este mecanismul de asigurare că CERTDIGITAL răspunde nevoilor clienților și altor părți interesate,
- ISO 27001 care demonstrează că firma utilizează un sistem de management al securității informațiilor de încredere
- Eliberarea pentru prelucrarea datelor personale în conformitate cu legislația Uniunii Europene (UE) și a României
- ISO 14001 care demonstrează că CERTDIGITAL a implementat și menține un sistem de management de mediu în conformitate cu acest standard;
- ISO 18001 care demonstrează că CERTDIGITAL a implementat și menține un Sistem de management al sănătății și securității în conformitate cu acest standard;