

**Declarația de transparență
a ierarhiei certSIGN ROOT CA G2**

Versiunea 2.28

Data: 15 Ianuarie 2026

**Notă
importantă**

Acest document este proprietatea certSIGN SA

Adresa: Bd. Tudor Vladimirescu, nr. 29 A,
AFI Tech Park 1, București 050881, România

Telefon: 004-021-31.19.901

Web: www.certsign.ro

certSIGN S.A.

Cod fiscal **RO18288250**, Registrul Comerțului: **J2006000484402**, EUID: **ROONRC.J2006000484402**, Capital social: **2.130.120,00 LEI**
Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București
Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro
ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR
ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Istoric document

Versione	Data efectivă	Motiv	Persoana care a făcut modificarea
1.0	28 Februarie 2017	Publicarea primei versiuni	Ofițer Securitate Informatică
2.0	15 Martie 2017	A doua versiune, după auditul intermediar	Ofițer Securitate Informatică
2.1	3 Aprilie 2017	Actualizare minoră pentru clarificare	Ofițer Securitate Informatică
2.2	14 August 2017	Actualizare minoră pentru clarificare	Ofițer Securitate Informatică
2.3	5 Februarie 2018	Revizuire anuală	Ofițer Securitate Informatică
2.4	25 Iunie 2018	Actualizare pentru adaugare profile certificate	Manager politici PKI
2.5	27 August 2018	Actualizare pentru adaugarea unei noi metode de identificare initiala	Manager politici PKI
2.6	25 Septembrie 2018	Semnatura la distanta cu RQSCD	Manager politici PKI
2.7	1 Noiembrie 2018	Actualizare pentru adaugare profile certificate simple, semnatura la distanta	Manager politici PKI
2.8	5 Noiembrie 2018	Actualizare determinata de schimbarea sediului	Manager politici PKI
2.9	14 Ianuarie 2019	Revizuire anuală	Manager politici PKI
2.10	9 Martie 2019	Actualizare pentru adaugare profile certificate (Trusted List)	Manager politici PKI
2.11	1 Aprilie 2019	Actualizare pentru adaugare profile certificate (dnQualifier)	Manager politici PKI
2.12	22 Iulie 2019	Actualizare pentru adaugare profile certificate (PSD2)	Manager politici PKI
2.13	30 Septembrie 2019	Actualizare minoră pentru clarificare (identificare cetățeni din afara RO)	Manager politici PKI
2.14	31 Ianuarie 2020	Revizuire anuală	Manager politici PKI
2.15	3 Februarie 2020	Actualizare pentru adaugare profile certificate calificate pentru sigilii	Manager politici PKI
2.16	15 Aprilie 2020	Actualizare răspundere certSIGN	Manager politici PKI
2.17	31 Iulie 2020	Adăugare OID cu pseudonim	Manager Politici PKI
2.18	7 Ianuarie 2021	Adăugare OIDs OUG 140/2020	Manager Politici PKI
2.19	29 Ianuarie 2021	Actualizare anuală	Manager Politici PKI
2.20	31 Ianuarie 2022	Actualizare anuală + OID protecție email	Manager Politici PKI
2.21	6 Octombrie 2022	Adăugare DV SSL	Manager Politici PKI
2.22	31 Ianuarie 2023	Revizuire anuală	Manager Politici PKI
2.23	31 Iulie 2023	Reduceri de OID-uri	Manager politici PKI
2.24	31 Ianuarie 2024	Revizuire anuală	Manager Politici PKI
2.25	15 Ianuarie 2025	Revizuire anuală	Manager Politici PKI
2.26	30 Aprilie 2025	Actualizare footer + EV	Manager Politici PKI
2.27	30 Octombrie 2025	Inlaturare OID 3.1.3.10	Manager Politici PKI
2.28	15 Ianuarie 2026	Revizuire anuală	Manager Politici PKI

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor și Procedurilor	Februarie 2017
2.0	Comitet de Management al Politicilor și Procedurilor	Martie 2017
2.1	Comitet de Management al Politicilor și Procedurilor	Aprilie 2017
2.2	Comitet de Management al Politicilor și Procedurilor	August 2017
2.3	Comitet de Management al Politicilor și Procedurilor	Februarie 2018
2.4	Comitet de Management al Politicilor și Procedurilor	Iunie 2018
2.5	Comitet de Management al Politicilor și Procedurilor	August 2018
2.6	Comitet de Management al Politicilor și Procedurilor	Septembrie 2018
2.7	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2018
2.8	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2018
2.9	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2019
2.10	Comitet de Management al Politicilor și Procedurilor	Martie 2019
2.11	Comitet de Management al Politicilor și Procedurilor	Aprilie 2019
2.12	Comitet de Management al Politicilor și Procedurilor	Iulie 2019
2.13	Comitet de Management al Politicilor și Procedurilor	Septembrie 2019
2.14	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2020
2.15	Comitet de Management al Politicilor și Procedurilor	Februarie 2020
2.16	Comitet de Management al Politicilor și Procedurilor	Aprilie 2020
2.17	Comitet de Management al Politicilor și Procedurilor	Iulie 2020
2.18	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2021
2.19	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2021
2.20	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2022
2.21	Comitet de Management al Politicilor și Procedurilor	Octombrie 2022
2.22	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2023
2.23	Comitet de Management al Politicilor și Procedurilor	Iulie 2023
2.24	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2024
2.25	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2025
2.26	Comitet de Management al Politicilor și Procedurilor	Aprilie 2025
2.27	Comitet de Management al Politicilor și Procedurilor	Octombrie 2025
2.28	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2026

Cuprins

1	DATE DE CONTACT CERTSIGN.....	6
2	TIPUL CERTIFICATULUI, PROCEDURI DE VALIDARE ȘI UTILIZARE.....	7
3	LIMITAREA ÎNCREDERII	18
4	OBLIGATIILE BENEFICIARILOR	18
5	OBLIGAȚIILE ENTITĂȚILOR PARTENERE DE A VERIFICA STAREA CERTIFICATULUI.....	19
6	GARANȚIE LIMITATĂ & DECLINAREA / LIMITAREA RĂSPUNDERII	19
7	ACORDURI APLICABILE, CPP, POLITICA DE CERTIFICARE	19
8	POLITICA DE CONFIDENȚIALITATE	19
9	POLITICA DE RAMBURSARE.....	20
10	LEGEA APLICABILĂ, PLÂNGERILE ȘI REZOLVAREA DISPUTELOR	20
11	LICENȚE DEPOZITAR ȘI TSA, MĂRCI DE ÎNCREDERE ȘI AUDIT.....	20

1 Date de contact certSIGN

Date de contact:

certSIGN S.A.

Adresa: Bd. Tudor Vladimirescu, nr. 29A, AFI Tech Park 1, București 050881, România

Nr. Registrul Comerțului: J2006000484402

Cod Înregistrare Fiscală: RO 18288250

Site: www.certsign.ro

Vânzări

Telefon: (+4031)1011870

E-mail: office@certsign.ro

Resurse Umane certSIGN

Telefon: (+4031)4133063 Int. 163

Suport tehnic

Telefon: (+4031)1011870

E-mail: suport@certsign.ro

Contact:

Telefon: (+4021)3119901

E-mail: office@certsign.ro

2 Tipul certificatului, proceduri de validare și utilizare

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

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

Nivel Root CA G2	Tip	Subtip
certSIGN ROOT CA G2	Certificate CA	Certificat certSIGN ROOT CA G2 Certificat certSIGN Public CA Certificat certSIGN Qualified CA Certificat certSIGN Web CA
certSIGN ROOT CA G2	Certificate OCSP	N/A

La Nivelul Sub CA al ROOT CA G2, certSIGN emite următoarele tipuri de certificate:

Sub CA al ROOT CA G2	Tip	Subtip
certSIGN Public CA	Certificate necalificate	<p><i>Din 2024 certSIGN Public CA NU a mai emis certificate – End-Of-Life</i></p> <p><i>Certificate ne-calificate pentru semnare si autentificare</i></p> <ul style="list-style-type: none"> ▪ Cu dispozitiv HW si cheie generata de certSIGN ▪ Cu dispozitiv HW si cheie generata si stocata de certSIGN pentru semnatura la distanta si autentificare ▪ Cu dispozitiv HW si cheie generata si stocata de certSIGN pentru semnatura la distanta si autentificare care poate fi folosita doar in relatia dintre Subiect si Beneficiar ▪ Fara dispozitiv HW si cheie generata de certSIGN ▪ Cu dispozitiv HW și cheie generată și stocată de certSIGN pentru semnătură la distanță, cu pseudonim <p><i>Certificate ne-calificate pentru criptare</i></p> <ul style="list-style-type: none"> ▪ Cu dispozitiv HW si cheie generata de certSIGN ▪ Fara dispozitiv HW si cheie generata de certSIGN <p><i>Certificate necalificate pentru sigiliu</i></p> <ul style="list-style-type: none"> ▪ Cu dispozitiv HW si cheie generata de certSIGN ▪ Cu dispozitiv HW si cheie generata si stocata de certSIGN pentru sigiliu la distanta ▪ Fara dispozitiv HW si cheie generata de certSIGN <p><i>Certificate OCSP</i></p>

Sub CA al ROOT CA G2	Tip	Subtip
certSIGN Qualified CA	Certificate calificate	<p><i>Din 2024 certSIGN Qualified CA NU a mai emis certificate – End-Of-Life</i></p> <p><i>Certificate calificate pentru semnare</i></p> <ul style="list-style-type: none"> ▪ cu QSCD si cheie generata de Subiect ▪ cu QSCD si cheie generata de certSIGN <ul style="list-style-type: none"> ○ cu QSCD si cheie generata si stocata de certSIGN pentru semnatura la distanta ○ cu QSCD si cheie generata si stocata de certSIGN pentru semnatura la distanta care poate fi folosita doar in relatia dintre subiect si beneficiar ▪ fara QSCD si cheie generata de certSIGN ▪ Conform OUG 140/2020 cu QSCD ▪ Conform OUG 140/2020 cu QSCD și cheie generată și stocată de certSIGN pentru semnătură la distanță <p><i>Certificate calificate pentru sigiliu</i></p> <ul style="list-style-type: none"> ▪ cu QSCD si cheie generata de certSIGN ▪ cu QSCD și cheie generata si stocata de certSIGN pentru sigiliu la distanta ▪ fara QSCD si cheie generata de certSIGN ▪ fara QSCD și cheie generata si stocata de certSIGN pentru pentru Prestatorii de servicii de plati conform Directivei UE/PSD2 <p><i>Certificat server pentru marcare temporală</i></p> <p><i>Certificat OCSP</i></p>
certSIGN Web CA	Certificate servere web	<p><i>Certificat calificat pentru autentificarea site-urilor Web (QWAC)</i></p> <p><i>Certificat calificat pentru autentificarea site-urilor Web pentru prestatori de servicii de plati în conform Directivei UE (QWAC PSD2)</i></p> <p><i>Certificat necalificat pentru autentificarea site-urilor Web – cu Validare Extinsa (EV)</i></p> <p><i>Certificat necalificat pentru autentificarea site-urilor Web – cu Validarea Organizației (OV)</i></p> <p><i>Certificat necalificat pentru autentificarea site-urilor Web – cu Validarea Domeniului (DV)</i></p> <p><i>Certificat OCSP</i></p>

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

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
Certificat calificat pentru semnatura electronica	Pentru semnatura electronica Din 2024 certSIGN Qualified CA NU a mai emis certificate – End-Of-Life	Cu QSCD și cheie generată de Subiect CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.1 Aceasta politică se conformează prevederilor ETSI EN 319 411-2	Persoana fizica se obliga sa prezinte la cererea autoritatii de inregistrare urmatoarele documente: <ul style="list-style-type: none"> • Acord contractual • Termeni si conditii • Documente de identificare (act de identitate sau pașaport, în cazul cetățenilor români; act de identitate, pașaport sau un document de identitate emis de Autoritățile Române, în cazul cetățenilor străini) care confirmă identitatea Subiectului, Și dacă Subiectul sau Beneficiarul dorește să includă datele unei instituții (entitate juridică) pentru care lucrează: <ul style="list-style-type: none"> • Extrasul valid de la Registrul Comerțului (sau echivalentul, pentru societățile străine înregistrate conform legislației străine); • Extras din Registrul asociațiilor și fundațiilor (sau echivalent pentru asociațiile și fundațiile străine) • Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este reprezentantul legal al entității • În cazul entităților fără personalitate juridică, identificarea Subiectului se va face în baza actului normativ de înființare • certSIGN verifica si relatia contractuala a Beneficiarului cu Subiectii.
		Cu QSCD și cheie generată de certSIGN CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.2 Aceasta politică se conformează prevederilor ETSI EN 319 411-2	
		Cu QSCD si cheie generata si stocata de certSIGN pentru semnatura la distanta CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.2.1 Aceasta politică se conformează prevederilor ETSI EN 319 411-2	
		Cu QSCD si cheie generata si stocata de certSIGN pentru semnatura la distanta care poate fi folosita doar in relatia dintre Subiect si Beneficiar CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.2.2 Aceasta politică se conformează prevederilor ETSI EN 319 411-2	

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
		<p>Fără QSCD și cheie generată de certSIGN CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.9 Aceasta politică se conformează prevederilor ETSI EN 319 411-2</p> <p>Conform OUG 140/2020 cu QSCD CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.14 Aceasta politică se conformează prevederilor ETSI EN 319 411-2</p> <p>Conform OUG 140/2020 cu QSCD și cheie generată și stocată de certSIGN pentru semnătură la distanță CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.15 Aceasta politică se conformează prevederilor ETSI EN 319 411-2</p>	<p>Identificarea trebuie făcută față-în-față sau prin metode de identificare ce oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică, în fața unui notar public sau prin utilizarea unui certificat calificat emis numai de certSIGN.</p>
<p>Certificat calificat pentru sigiliu electronic</p>	<p>Pentru sigiliu electronic</p> <p>Din 2024 certSIGN Qualified CA NU a mai emis</p>	<p>Cu QSCD și cheie generată de certSIGN CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.4 Aceasta politică se conformează prevederilor ETSI EN 319 411-2</p> <p>Cu QSCD și cheie generată de certSIGN pentru sigiliu la distanță</p>	<p>Reprezentanții autorizați ai instituției sunt obligați să prezinte, la cererea Autorității de Înregistrare, următoarele documente:</p> <ul style="list-style-type: none"> • Acord contractual • Termeni și condiții • Extrasul valid de la Registrul Comerțului (sau echivalentul, pentru societățile străine înregistrate conform legislației străine);

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
	certificate – End-Of-Life	CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.4.1 Aceasta politica se conformează prevederilor ETSI EN 319 411-2	<ul style="list-style-type: none"> Extras din Registrul asociațiilor și fundațiilor (sau echivalent pentru asociațiile și fundațiile străine) Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este reprezentantul legal al entității
		Fara QSCD și cheie generata de certSIGN pentru sigiliu la distanta CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.12 Aceasta politica se conformează prevederilor ETSI EN 319 411-2	<ul style="list-style-type: none"> În cazul entităților fără personalitate juridică, identificarea Subiectului se va face în baza actului normativ de înființare <p>Identificarea trebuie făcută față-în-față sau prin metode de identificare ce oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică, in fata unui notar public sau prin utilizarea unui certificat calificat emis numai de certSIGN.</p>
		Fara QSCD și cheie generata de certSIGN pentru Prestatorii de servicii de plati conform Directivei UE/PSD2 CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.13 Aceasta politica se conformează prevederilor ETSI EN 319 411-2	
Certificat de server pentru marcarea temporală	Doar pentru semnarea token-urilor de marcarea temporală	Timestamp CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.5 Aceasta politica se conformează prevederilor ETSI EN 319 411-2	Vezi certificat calificat pentru sigiliul electronic.
OCSP Certificate	Doar pentru semnarea	OCSP CPP certSIGN CA Calificat OID: 1.3.6.1.4.1.25017.3.1.3.6	Vezi certificat calificat pentru sigiliul electronic

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
	răspunsurilor OCSP	Aceasta politică se conformează prevederilor ETSI EN 319 411-2	
Certificat ne-calificat pentru autentificare și semnare	Pentru semnătură electronică și autentificare Din 2024 certSIGN Public CA NU a mai emis certificate – End-Of-Life	<p>Cu dispozitiv HW și cheie generată de certSIGN CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.3 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p> <p>Cu dispozitiv HW si cheie generata si stocata de certSIGN pentru semnatura la distanta si autentificare CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.3.1 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p> <p>Cu dispozitiv HW si cheie generata si stocata de certSIGN pentru semnatura la distanta si autentificare care poate fi folosita doar in relatia dintre Subiect si Beneficiar CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.3.2 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p>	<p>Persoana fizica se obliga sa prezinte la cererea autoritatii de inregistrare urmatoarele documente:</p> <ul style="list-style-type: none"> • Acord contractual • Termeni si conditii, • Documente de identitate (act de identitate sau pașaport, în cazul cetățenilor români, pașaport în cazul cetățenilor străini și pașaport sau un document de identitate emis de Autoritățile Române, în cazul cetățenilor străini care au drept de ședere pe teritoriul României) care confirmă identitatea subiectului, <p>Și dacă Subiectul sau Beneficiarul dorește să includă datele unei instituții (entitate juridică) pentru care lucrează:</p> <ul style="list-style-type: none"> • Documentele oficiale care demonstrează că persoana juridică acționează ca angajator al persoanei fizice sau că există un juridic între ele. <p>Nu este necesară identificarea față-în-față.</p>

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
		<p>Fără dispozitiv HW și cheie generată de certSIGN CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.4 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p>	
<p>Certificat ne-calificat pentru autentificare și semnare</p>	<p>Pentru semnătură electronică și autentificare Din 2024 certSIGN Public CA NU a mai emis certificate – End-Of-Life</p>	<p>Cu dispozitiv HW și cheie generată și stocată de certSIGN pentru semnătură la distanță și autentificare, cu pseudonim CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.14 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p>	<p>Subiectul declară un pseudonim, email și număr de telefon, și acceptă termenii și condițiile specifice. Se verifică doar telefonul.</p>
<p>Certificate ne-calificate pentru sigiliu electronic</p>	<p>Doar pentru sigiliu electronic Din 2024 certSIGN Public CA NU a mai emis</p>	<p>Cu dispozitiv HW și cheie generată de certSIGN CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.11 Cu dispozitiv HW și cheie generată și stocată de certSIGN pentru sigiliu la distanță CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.11.1 Aceste politici se conformează prevederilor ETSI EN 319 411-1</p>	<p>Reprezentanții autorizați ai instituției sunt obligați să prezinte, la cererea Autorității de Înregistrare, următoarele documente:</p> <ul style="list-style-type: none"> • Contract, • Termeni și condiții, • Extras valid de la registrul comerțului (sau echivalentul străin al societăților străine înregistrate sub incidența dreptului străin);

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
	certificate – End-Of-Life	<p>Fără dispozitiv HW și cheie generată de certSIGN CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.12 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p>	<ul style="list-style-type: none"> Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este administratorul legal al entității. Documente care atestă identitatea subiectului (carte de identitate sau pașaport, în cazul cetățenilor români, pașaport în cazul cetățenilor străini și pașaport sau un document de identitate emis de Autoritățile Române, în cazul cetățenilor străini care au drept de ședere pe teritoriul României); <p>Nu este necesară identificarea față-în-față.</p>
Certificate ne-calificate pentru criptare	Doar pentru criptarea datelor Din 2024 certSIGN Public CA NU a mai emis certificate – End-Of-Life	<p>Cu dispozitiv HW și cheie generată de certSIGN CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.7 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p> <p>Fără dispozitiv și cheie generată de certSIGN CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.8 Aceasta politică se conformează prevederilor ETSI EN 319 411-1</p>	Vezi certificate ne-calificate pentru autentificare și semnare

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
Certificat OCSP	Doar pentru semnarea răspunsurilor OCSP	OCSP CPP certSIGN Public CA OID:1.3.6.1.4.1.25017.3.1.2.13 Aceasta politică se conformează prevederilor ETSI EN 319 411-1	Vezi certificate ne-calificate pentru sigiliu electronic.
Certificat pentru autentificare a organizației site-urilor Web (OV SSL)	Doar pentru autentificare a serverelor Web	Certificat pentru autentificarea site-urilor Web (OV SSL) CPP certSIGN Web CA pentru SSL OV OID: 1.3.6.1.4.1.25017.3.1.4.2 Aceasta politica se conformeaza prevederilor ETSI EN 319 411-1 si cerintelor CAB Forum Baseline	Organizațiile românești sunt autentificate pe baza unor documente și atestări recente, valabile în România. Organizațiile din alte țări ale UE fiind autentificate pe baza documentelor și atestărilor echivalente aplicabile țării în cauză. Reprezentanții autorizați ai organizației sunt obligați să prezinte la solicitarea Autorității de înregistrare următoarele documente: <ul style="list-style-type: none"> • Copie certificată „conform cu originalul” a certificatului de înregistrare a companiei; • Documente care atestă identitatea solicitantului (act de identitate sau pașaport) și împuternicirea care să confirme că este reprezentantul companiei; • Cerere de cumpărare; • Declarație standard a proprietarului domeniului Procedura pe care RA o aplică pentru verificarea identității persoanei juridice și a reprezentanților autorizați ai acesteia constă în: <ul style="list-style-type: none"> • Verificarea documentelor prezentate de Beneficiar, • Verificarea cererii, care constă în: <ul style="list-style-type: none"> ○ Verificarea conformității datelor specificate in cerere cu cele din documentele prezentate, ○ Verificarea dovezii de deținere a cheii private si a faptului că Distinctive Name este cel potrivit,

certSIGN S.A.

Cod fiscal **RO18288250**, Registrul Comerțului: **J2006000484402**, EUID: **ROONRC.J2006000484402**, Capital social: **2.130.120,00 LEI**

Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București

Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro

ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR

ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
			<ul style="list-style-type: none"> o Verificarea autorizării și a identității reprezentantului persoanei juridice care depune cererea în numele entității.
Certificat pentru autentificare a domeniului site-urilor Web (DV SSL)	Doar pentru autentificare a serverelor Web	Certificat pentru autentificarea site-urilor Web (DV SSL) CPP certSIGN Web CA pentru SSL DV OID: 1.3.6.1.4.1.25017.3.1.4.5 Aceasta politica se conformeaza prevederilor ETSI EN 319 411-1 si cerintelor CAB Forum Baseline	Conform CA/B Forum BR Guidelines (www.cabforum.org) sectiunea 3 și 4.
Certificat pentru autentificare extinsa a domeniului site-urilor Web (EV SSL)	Doar pentru autentificare a serverelor Web	Certificat pentru autentificarea extinsa a site-urilor Web (EV SSL) CPP certSIGN Web CA pentru SSL EV-QWAC OID: 1.3.6.1.4.1.25017.3.1.4.6 Aceasta politica se conformeaza prevederilor ETSI EN 319 411-1 si cerintelor CAB Forum BR si EV	Conform CA/B Forum BR Guidelines (www.cabforum.org) sectiunea 3 și 4. Conform CA/B Forum EV Guidelines (www.cabforum.org) sectiunea 3 și 4.
Certificat calificat pentru autentificare Web (QWAC SSL)	Doar pentru autentificare a serverelor Web	Certificat calificat pentru autentificarea site-urilor Web (QWAC SSL) CPP certSIGN Web CA pentru certificate calificate pentru autentificarea site-urilor Web OID: 1.3.6.1.4.1.25017.3.1.4.1 Aceasta politica se conformeaza prevederilor ETSI EN 319 411-2 si cerintelor CA/B Forum EV	Conform CA/B Forum EV Guidelines (www.cabforum.org) sectiunea 3 și 4
		Certificat calificat pentru autentificarea site-urilor Web pentru Prestatorii de servicii de	Conform CA/B Forum EV Guidelines (www.cabforum.org) sectiunea 3 și 4

Tip/subtip certificat	Utilizare	Politica de certificare	Procedura de validare
		<p>plăți conform Directivei UE/PSD2 (QWAC/PSD2) CPP certSIGN Web CA pentru certificate calificate pentru autentificarea site-urilor Web OID: 1.3.6.1.4.1.25017.3.1.4.4 Aceasta politica se conformeaza prevederilor ETSI EN 319 411-2 si cerintelor CA/B Forum EV</p>	
Certificat OSCP	Doar pentru semnarea raspunsurilor OSCP	<p>OCSP CPP certSIGN Web CA pentru SSL OV OID: 1.3.6.1.4.1.25017.3.1.4.3 Aceasta politica se conformeaza prevederilor ETSI EN 319 411-1 si cerintelor CAB Forum Baseline</p>	Vezi Web Server certificate OV SSL

certSIGN S.A.

Cod fiscal **RO18288250**, Registrul Comerțului: **J2006000484402**, EUID: **ROONRC.J2006000484402**, Capital social: **2.130.120,00 LEI**

Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București

Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro

ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR

ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

3 Limitarea Încrederii

certSIGN va acoperi despăgubirile pe care le-ar putea provoca prin prestarea serviciilor de certificare persoanelor care își întemeiază conduita pe 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.

certSIGN va acoperi daunele-interese pe care le-ar putea provoca prin prestarea serviciilor de certificare persoanelor care își întemeiază conduita pe efectele juridice ale certificatelor calificate pentru certificate de autentificare a site-urilor web (QWAC SSL) conform cerințelor CAB Forum EV.

4 Obligatiile beneficiarilor

Beneficiarii se angajează să:

- Respecte regulile acordului încheiat cu certSIGN;
- Utilizeze numai perechile de chei pentru scopurile definite în secțiunea 2 de mai sus și în conformitate cu orice alte limitări care pot fi notificate Beneficiarului;
- Prezinte sau să transmita documentele necesare care să confirme informațiile incluse în cererea de certificare;
- Exerce o atenție rezonabilă pentru a evita utilizarea neautorizată a cheii private a subiectului.
- Notifice certSIGN, fără întârzieri nejustificate, dacă apare oricare dintre situațiile următoare până la sfârșitul perioadei de valabilitate indicate în Certificat:
 - Cheia privată a subiectului a fost pierdută, furată sau compromisă,
 - 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,
 - Inexactități sau modificări ale conținutului certificatului, astfel cum este notificat Beneficiarului.
- Se asigure că, dacă Beneficiarul sau Subiectul generează perechile de chei ale Subiectului, numai Subiectul deține cheia privată,
- Utilizeze certificatul și cheia privată corespunzătoare numai în scopul menționat în certificat și în conformitate cu scopurile și restricțiile enunțate în acest document.

5 Obligațiile Entităților Partenere de a verifica starea certificatului

Entitățile partenere, trebuie să utilizeze toate resursele pe care certSIGN le pune la dispoziție prin depozitarul său pentru a verifica starea unui certificat în orice moment înainte de a se baza pe acesta. CertSIGN actualizează OCSP și CRL-urile în consecință.

6 Garanție limitată & declinarea / limitarea răspunderii

În limitele stabilite de legea română, certSIGN nu va răspunde în niciun caz (cu excepția fraudelor sau a faptelor ilicite săvârșite cu intenție) pentru:

- Orice pierderi de profit;
- Orice pierderi de date;
- Orice daune indirecte, subsecvente sau punitive ce decurg din sau în legătură cu utilizarea, livrarea, licența și performanța sau non-performanța certificatelor sau a semnăturilor electronice;
- Orice alte daune.

În pofida celor de mai sus, dacă certSIGN nu a emis sau gestionat certificatul în conformitate cu cerințele de bază și cu politica de certificare, certSIGN acoperă orice daune directe aduse Beneficiarilor sau părților, care se bazează pe certificate pentru o creanță recunoscută și probată, până la o sumă de două mii de dolari SUA per Beneficiar sau Entitate Parteneră.

7 Acorduri aplicabile, CPP, Politica de certificare

certSIGN publică în Depozitarul disponibili la <https://www.certsign.ro/ro/depozitar/> următoarele documente:

- CPP al **certSIGN ROOT CA G2**
- CPP al **certSIGN CA Calificat**
- CPP al **certSIGN Public CA**
- CPP al **certSIGN Web CA** pentru certificate SSL DV
- CPP al **certSIGN Web CA** pentru certificate SSL OV
- CPP al **certSIGN Web CA** pentru certificate pentru autentificarea site-urilor web (EV-QWAC SSL)

8 Politica de confidențialitate

Toate informațiile au fost obținute, păstrate și procesate în conformitate cu legile aplicabile, în mod special cu Regulamentul UE 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și cu Legea nr. 190/2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și cu orice norme general obligatorii adoptate în legătură cu protecția datelor cu caracter personal. Relațiile dintre un Beneficiar, o Entitate Parteneră și certSIGN se bazează pe încredere.

9 Politica de rambursare

Politica de rambursare este definită în politica internă de preț. Dacă un Beneficiar sau Entitate Parteneră nu este satisfăcut de servicii, poate cere rambursarea taxei, doar dacă *certSIGN nu își îndeplinește obligațiile* și îndatoririle specificate în Acordul cu Beneficiarul și în prezentul document și în conformitate cu legea română.

10 Legea aplicabilă, plângerile și rezolvarea disputelor

Legile române vor reglementa aplicabilitatea, construirea, interpretarea și valabilitatea prezentului document (fără a crea niciun conflict cu prevederile legale care ar determina aplicarea altor legi).

certSIGN respectă Legea Română nr.214/2024 - privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea.

11 Licențe Depozitar și TSA, Mărci de Încredere și Audit

CA emite certificate utilizând produsele dezvoltate intern de certSIGN și care au fost acreditate de NATO (Catalogul NATO - NIAPC) și de către Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNIS) ca fiind capabile să protejeze informațiile CLASIFICATE.

În furnizarea serviciilor de încredere, certSIGN deține mai multe acreditări și certificări. Acestea includ:

- Webtrust for Certification Authorities – realizată anual de Ernst&Young, această certificare asigură potențialele Entități Partenere că un specialist calificat a evaluat controalele și practicile de business ale Autorității de Certificare pentru a determina dacă ele respect Principiile și Criteriile AICPA/CICA WebTrust Principles and Criteria pentru Autoritățile de Certificare, și a emis un raport cu o opinie fără rezerve care indică respectarea acelor principii.
- ISO/IEC 20000-1, care certifică faptul că Sistemul de Management al Serviciului IT operat de certSIGN este în conformitate cu acest standard, pentru furnizarea următoarelor servicii: dezvoltarea și întreținerea de software și sisteme informatice; Securitatea cibernetică (de exemplu, răspunsul la incidente și analiza, evaluarea vulnerabilității și testarea penetrării, Advanced Threat Intelligence & Correlation);
- ISO 9001, care demonstrează implementarea unui sistem de management al calității, ce reprezintă mecanismul care asigură că certSIGN răspunde nevoilor clienților și altor părți interesate, inclusiv pentru activitățile de instruire
- ISO 27001, care demonstrează utilizarea de către companie a unui Sistem de Încredere de Management al Securității informatice
- Permisivitatea de a procesa date cu caracter personal în conformitate cu legislația Uniunii Europene (UE) și cu legislația română
- ISO 14001 care demonstrează că certSIGN a implementat și menține un Sistem de Management de Mediu în conformitate cu acest standard;
- ISO 18001 care demonstrează că certSIGN a implementat și menține un Sistem de Management al Sănătății și securității în conformitate cu acest standard;

certSIGN S.A.

Cod fiscal **R018288250**, Registrul Comerțului: **J2006000484402**, EUID: **ROONRC.J2006000484402**, Capital social: **2.130.120,00 LEI**
Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București
Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro
ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR
ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA