PKI Disclosure Statement
for certSIGN ROOT CA G4 Hierarchy

Version 1.2

Date: 15 January, 2026

Important
Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date[1]	Reason	The person who made the change
1.0	15 July 2025	First draft version	PKI Policies Manager
1.1	19 August 2025	First version publishing	PKI Policies Manager
1.2	15 January 2026	Annual review	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
BU Trust Services	PKI Policies Manager	July 2025

Distribution List

Destination	Date distributed
Public-Internet	August 2025
Public-Internet	January 2026

This document was approved by:

Version	Name	Date
1.1	Policies and Procedures Management Body	August 2025
1.2	Policies and Procedures Management Body	January 2026

[1] Last day of the month, if not explicit

Content

1 certSIGN contact info

Contact Data:

CERTSIGN S.A.

Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania

Trade Commerce Registry no: J2006000484402

VAT Code: RO 18288250

Site

www.certsign.ro

Sales

Phone: (+4031)1011870

E-mail: office@certsign.ro

HR Certsign

Phone: (+4031)4133063 Int. 163

Technical support

Phone: (+4031)1011870

E-mail: suport@certsign.ro

Contact:

Phone: (+4021)3119901

E-mail: office@certsign.ro

2 Certificate type, validation procedures and usage

certSIGN issues the following types of certificates as described below.

At the ROOT CA G4 level, certSIGN issues the following types of certificates:

Root CA G4 Level	Type	Subtype
certSIGN ROOT CA G4	**CA certificates**	***certSIGN ROOT CA G4 certificate*** ***certSIGN Web CA G4 DV certificate*** ***certSIGN Web CA G4 OV certificate*** ***certSIGN Web CA G4 EV certificate***
certSIGN ROOT CA G4	**OCSP Certificate**	***N/A***

At the Sub CA Level of Root CA G4, certSIGN issues the following types of certificates:

Sub CA Level of ROOT CA G4	Type	Certificate Type
certSIGN Web CA G4 DV	**Web servers certificate**	***Domain Validated Website Authentication Certificate (DV)*** ***OCSP certificate***
certSIGN Web CA G4 OV	**Web servers certificate**	***Organization Validated Website Authentication Certificate (OV)*** ***OCSP certificate***
certSIGN Web CA G4 EV	**Web servers certificate**	***Extended Validation Website Authentication Certificate (EV)*** ***Qualified Website Authentication Certificate (QWAC)*** ***Qualified Website Authentication Certificates for payment service providers in accordance with the EU Directive (QWAC PSD2)*** ***OCSP certificate***

certSIGN shall ensure that evidence of Subjects' identification and the accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized source, conforming to the following table:

Sub CA	Certificate type/subtype	Usage	Certification Policy	Validation procedure
certSIGN Web CA G4 DV	***Domain Validated Website Authentication Certificate (DV SSL)***	Only for Web server authentication	***Domain Validated Website Authentication Certificate (DV SSL)*** CPS certSIGN Web CA G4 DV **OID: 1.3.6.1.4.1.25017.10.1.1** This policy is conforming to ETSI EN 319 411-1 and CAB Forum Baseline requirements	Conforming to CA/B Forum BR Guidelines (www.cabforum.org) section 3 and 4
	OCSP Certificate	Only for signing OCSP responses	**OCSP** CPS certSIGN Web CA G4 DV **OID: 1.3.6.1.4.1.25017.10.1.2** This policy is conforming to ETSI EN 319 411-1 and CAB Forum Baseline requirements	The authorized representatives of certSIGN fill in a request form for the creation/renewal of the OCSP certificate. The request is approved by CIO/CISO and CEO.
certSIGN Web CA G4 OV	***Organization Validated Website Authentication Certificate (OV SSL)***	Only for Web server authentication	***Organization Validated Website Authentication Certificate (OV SSL)*** CPS certSIGN Web CA G4 OV **OID: 1.3.6.1.4.1.25017.10.2.1** This policy is conforming to ETSI EN 319 411-1 and CAB Forum Baseline requirements	Romanian organizations are authenticated based on recent documents and attestations, which are valid in Romania, organizations from other EU countries, are authenticated based on the equivalent documents and attestations as applicable for the country in question. The authorized representatives of the organization are bind to present upon the request of the Registration Authority the following documents: • Certified copy „in compliance with the original" of the registration certificate of the company; • Documents to attest the Applicant's identity (identity card or passport) and

Sub CA	Certificate type/subtype	Usage	Certification Policy	Validation procedure
				the authorization attesting that he is representing the company; • Purchasing request; • Template statement of the domain's owner The procedure performed by RA to verify the legal entity's identity and its authorized representative's identity consists of: ▪ Verify the documents presented by the Subscriber, ▪ Verify the request, that consists of: o Verifying the compliance of the data mentioned in the request with those from the documents presented, o verifying the proof of private key possession and the fact that the Distinctive Name is the right one, o Verifying the authorization and identity of the representative of the legal entity that submits the request on behalf of this entity
	OCSP Certificate	Only for signing OCSP responses	**OCSP** CPS certSIGN Web CA G4 OV **OID: 1.3.6.1.4.1.25017.10.2.2** This policy is conforming to ETSI EN 319 411-1 and CAB Forum Baseline requirements	The authorized representatives of certSIGN fill in a request form for the creation/renewal of the OCSP certificate. The request is approved by CIO/CISO and CEO.

Sub CA	Certificate type/subtype	Usage	Certification Policy	Validation procedure
certSIGN Web CA G4 EV	***Extended Validation Website Authentication Certificate (EV SSL)***	Only for Web server authentication	***Extended Validation Website Authentication Certificate (EV SSL)*** CPS certSIGN Web CA G4 EV **OID: 1.3.6.1.4.1.25017.10.3.1** This policy is conforming to ETSI EN 319 411-1 and CAB Forum Baseline & EV requirements	Conforming to CA/B Forum BR Guidelines (www.cabforum.org) section 3 and 4. Conforming to CA/B Forum EV Guidelines (www.cabforum.org) section 3 and 4
	Qualified Website Authentication Certificate (QWAC SSL)	Only for Web server authentication	***Qualified Website Authentication Certificate (QWAC SSL)*** CPS certSIGN Web CA G4 EV **OID: 1.3.6.1.4.1.25017.10.3.2** This policy is conforming to ETSI EN 319 411-2 and CA/B Forum EV Guidelines	Conforming to CA/B Forum EV Guidelines (www.cabforum.org) section 3 and 4
			Qualified Website Authentication Certificate for payment service providers in accordance with the EU Directive/PSD2 (QWAC/PSD2) CPS certSIGN Web CA G4 EV **OID: 1.3.6.1.4.1.25017.10.3.3** This policy is conforming to ETSI EN 319 411-2 and CA/B Forum EV Guidelines	Conforming to CA/B Forum EV Guidelines (www.cabforum.org) section 3 and 4
	OCSP Certificate	Only for signing OCSP responses	**OCSP** CPS certSIGN Web CA G4 EV **OID: 1.3.6.1.4.1.25017.10.3.4** This policy is conforming to ETSI EN 319 411-1 and CAB Forum Baseline requirements	The authorized representatives of certSIGN fill in a request form for the creation/renewal of the OCSP certificate. The request is approved by CIO/CISO and CEO.

3 Reliance Limits

certSIGN will cover the damages that could be caused by providing certification services to persons who base their conduct on the legal effects of qualified certificates up to the equivalent in lei of EUR 10,000 for each insured risk. The insured risk represents every damage caused even if there are more such damages after the provider failed to fulfil the liabilities mentioned by law.

certSIGN will cover damages it might cause by providing certification services for persons that build their moral on the legal effects of the **Qualified certificates for Website authentication (QWAC SSL) certificates** conforming to CA/B Forum EV Guidelines requirements.

4 Obligations of the Subscribers

Subscribers are committed to:

- comply with the rules of the agreement made with certSIGN;
- only use the Key Pairs for the purposes defined in Section 2 above and in accordance with any other limitations that may be notified to the Subscriber;
- submit or present of required documents confirming the information included in a certification request;
- exercise reasonable care to avoid unauthorized use of the Subject's Private Key
- notify certSIGN, without any unreasonable delay, if any of the following occurs up to the end of the validity period indicated in the Certificate:
  - the Subject's Private Key has been potentially or lost, stolen or compromised
  - control over the Subject's Private Key has been lost due to potential or actual compromise of activation data (e.g. PIN code) or other reasons
  - Inaccuracy or changes to the Certificate content, as notified to the Subscriber.
- ensure that if the Subscriber or Subject generates the Subject's Key Pair, only the Subject holds the Private Key
- apply the certificate and the corresponding private key only for the purpose stated in the certificate and in accordance with the aims and restrictions stated in this document

5 Obligations of the relying parties for the verification of the certificate status

Relying Parties must use all the resources that certSIGN makes available through its repository to check the status of a Certificate any time before relying on it. certSIGN updates OCSP, CRLs accordingly.

6 Limited warranty & disclaimer/ limitation of liability

Within the limit set by the Romania Law, in no event (except for fraud or wilful misconduct) certSIGN will be liable for:

- Any loss of profits;
- Any loss of data;

- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;
- Any other damages.

Notwithstanding the above, if Certsign has not issued or managed the Certificate in compliance with the Baseline Requirements and its Certificate Policy and/or Certification Practice Statement, Certsign shall cover any direct damage to Subscribers or Relying Parties for legally recognized and provable claims limited to a monetary amount of two thousand US dollars per Subscriber or Relying Party per Certificate.

7 Applicable agreements, certification practice statement, certificate policy

certSIGN publishes at the repository https://www.certsign.ro/en/repository/ the following documents:

- Certification Practice Statement of **certSIGN ROOT CA G4**
- Certification Practice Statement of **certSIGN Web CA G4 DV** for DV TSL certificates
- Certification Practice Statement of **certSIGN Web CA G4 OV** for OV TSL certificates
- Certification Practice Statement of **certSIGN Web CA G4 EV** for TLS certificates for Website Authentication (EV or QWAC or QWAC-PSD2 TLS)

8 Privacy policy

All certSIGN's information was gathered, stored and processed in compliance with applicable laws, mainly with EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Law no. 190/2018 regarding the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any generally binding rules adopted in relation to the protection of personal data. Relations between a Subject, Subscriber, Relying Party and certSIGN are based on trust.

9 Refund Policy

Refund policy is defined within the internal price policy. If a subscriber or a relying party is not satisfied with the services, they may request certificate revocation and fee refund only if certSIGN does not fulfil its obligations and duties specified in the subscriber agreement and the present document and according with Romanian Law.

10 Applicable law, complaints and dispute resolution

The Romanian laws shall govern the enforceability, construction, interpretation, and validity of the present document (without giving effect to any conflict of law provision that would cause the application of other laws).

certSIGN complies with Romanian Law no.214/2024 on the use of electronic signatures, time-stamping and the provision of trust services based on them.

11 Certificate Authority and Repository Licenses, Trust Marks and Audit

The CA issues Certificates using certSIGN internal developed products that have been accredited by NATO (NATO Catalogue - NIAPC) and by Romanian National Security Agency (ORNISS) as being capable to protect CLASSIFIED information.

In the provision of trust services, certSIGN maintains several accreditations and certifications. These include:

- eIDAS Trust Services audit – annually performed by LSTI, for almost all PKI Systems and Services. This certification ensures the National Supervisory Body and the potential relying parties that certSIGN, as a Qualified Trust Services Provider, has proven that it's business practices and it's procedural and technical controls are in conformity with the eIDAS Regulations and latest ETSI standards.
- Webtrust for Certification Authorities – annually performed by Crowe, for a distinct PKI System, this certification ensures the potential relying parties that a qualified practitioner has evaluated Certification Authority's business practices and control to determine whether they are in conformity with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities, and has issued a report with an unqualified opinion indicating that those principles are respected.
- ISO/IEC 20000-1, certifying that the Information Technology Service Management System operated by certSIGN is in compliance with this standard, for the provision of the following services: developing and maintenance for software and information systems; cybersecurity (e.g.: incident response and analysis, vulnerability assessment and penetration testing, Advanced Threat Intelligence & Correlation);
- ISO 9001 demonstrating the implementation of a quality management system, which is the ensuring mechanism that certSIGN meets the needs of customers and other stakeholders, also for training activities
- ISO 27001 demonstrating that the company is using a trusted Information security management system
- Clearance for personal data processing according to European Union (EU) and Romanian legislation
- ISO 14001 demonstrating that certSIGN has implemented and maintains an Environmental Management System according to this standard;
- ISO 18001 demonstrating that certSIGN has implemented and maintains a Health and Safety Management System according to this standard.