PKI Disclosure Statement
for certSIGN ROOT CA G3 Hierarchy

Version 1.4

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	Reason	The person who made the change
1.0	15 December 2022	First version publishing	PKI Policies Manager
1.1	09 March 2023	Minor updates (title)	PKI Policies Manager
1.2	31 January 2024	Annual review	PKI Policies Manager
1.3	15 January 2025	Annual review	PKI Policies Manager
1.4	15 January 2026	Annual review	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
certSIGN	PKI Policies Manager	December 2022

Distribution List

Destination	Date distributed
Public-Internet	December 2022
Public-Internet	March 2023
Public-Internet	January 2024
Public-Internet	January 2025
Public-Internet	January 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	December 2022
1.1	Policies and Procedures Management Body	March 2023
1.2	Policies and Procedures Management Body	January 2024
1.3	Policies and Procedures Management Body	January 2025
1.4	Policies and Procedures Management Body	January 2026

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 G3 level, CERTSIGN issues the following types of certificates:

ROOT CA G3 Level	Type	Subtype

certSIGN ROOT CA G3	**CA certificates**	• ***certSIGN ROOT CA G3 certificate***
		• ***CADef CA certificate***
		• ***Closed circuit CAs, in end-of-life:***
		  • *certSIGN FOR BNR SIMPLE SSL PRODUCTION CA*
		  • *certSIGN FOR BNR QUALIFIED DS TEST CA*
		  • *certSIGN FOR BNR SIMPLE SSL TEST CA*
		  • *certSIGN FOR BNR QUALIFIED DS PRODUCTION CA*

	OCSP certificate	***N/A***

At the Sub CA Level of ROOT CA G3, CERTSIGN issues the following types of certificates:

Sub CA Level of ROOT CA G3	Type	Subtype
certSIGN CADef CA	**Qualified certificates**	***Qualified certificate for electronic signature*** ▪ with QSCD and key generated by Subject
	OCSP certificate	***N/A***
certSIGN FOR BNR CA		***NOT issuing any end-user certificates – end-of-life CAs***

certSIGN will 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:

Certificate type/subtype	Usage	Certification Policy	Validation procedure
Qualified certificate for electronic signature	For electronic signature	***With QSCD and key generated by the Subject*** CPS certSIGN CADef CA **OID: 1.3.6.1.4.1.25017.6.1.1** This policy is conforming to ETSI EN 319 411-2	The natural person is bound to present upon the request of the Registration Authority the following documents: • Subscriber agreement • Terms and conditions • Identity documents (identity card or passport, for Romanian citizens; ID Card, passport or any other identity document issued by Romanian Authorities for foreign citizens) that confirms the Subject's identity, Identification shall be done face-to-face or by identification methods offering an equivalent level of assurance from the point of view of reliability with physical presence or public notary or by using a qualified certificate issued by CERTSIGN only, or remote through an ADR authorized third party.
OCSP Certificate	Only for signing OCSP responses	**OCSP** CPS certSIGN CADef CA **OID: 1.3.6.1.4.1.25017.6.1.3** This policy is conforming to ETSI EN 319 411-2	The requester for a OCSP certificate for a certSIGN CA, a certSIGN manager, transmits to the Registration Authority the following documents: • OCSP certificate request (CSR) signed by the requester, that is a certSIGN manager • Approval of issuing the OCSP certificate by certSIGN CIO, CTO, CEO or CISO

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.

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

To the extent permitted 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.

certSIGN shall not be liable to any person (beneficiary, subject, third party, partner entity, etc.) in the event that the data submitted when issuing certificates are false, inaccurate, incomplete or outdated or false identity documents are presented. certSIGN shall not be

liable for damages incurred by the Beneficiary or third parties caused by the use of certificates issued by certSIGN by the Subject.

In any case certSIGN's liability shall be limited to 200 euro per certificate and shall not exceed 10.000 euro in case of a claim, regardless of the number of certificates or the number of persons affected.

7 Applicable agreements, CPS, certificate policy

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

- Certification Practice Statement of **certSIGN ROOT CA G3**
- Certification Practice Statement of **CADef CA**

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:

- Webtrust for Certification Authorities – annually performed by Ernst&Young, 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.