

## INDEPENDENT ASSURANCE REPORT

To the management of CERTSIGN S.A.  
Certification Authority ("certSIGN")

30 April 2024

**Scope**

We have been engaged, in a reasonable assurance engagement, to report on certSIGN [management's assertion](#) that for its Certification Authority (CA) operations at Bucharest, Romania, throughout the period 2023-02-08 to 2024-02-07 for its Root CA with OU = certSIGN ROOT CA, O = certSIGN, C = RO, and 11 intermediate CA servers, certSIGN has:

(1) disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:

- [Certification Policy, certSIGN, Version 1.14 as of 31 January 2023,](#)
- [Certification Policy, certSIGN, Version 1.15 as of 31 July 2023,](#)
- [Certification Policy, certSIGN, Version 1.16 as of 31 January 2024,](#)
- [Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.39 as of 31 January 2023,](#)
- [Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.40 as of 31 July 2023,](#)
- [Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.41 as of 31 January 2024,](#)
- [Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.40, Date: 31 July 2023,](#)
- [Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.41, Date: 31 August 2023,](#)
- [Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.41a, Date: 31 January 2024,](#)
- [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.16 as of 31 January 2023,](#)
- [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.17 as of 15 May 2023,](#)
- [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.18 as of 31 July 2023,](#)
- [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19 as of 31 January 2024,](#)

- [Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.18, Date: 31 July 2023,](#)
  - [Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19, Date: 31 January 2024,](#)
  - Certification Practice Statement, certSIGN, SSL EV CA Class 3 G2 for SSL EV Certificates, Version 1.16 as of 31 January 2023 (retired),
  - Certification Practice Statement, certSIGN, SSL EV CA Class 3 G2 for SSL EV Certificates, Version 1.17 as of 31 July 2023 (retired on 2023-10-12).
- (2) maintained effective controls to provide reasonable assurance that:
- certSIGN Certification Practice Statements are consistent with its Certificate Policies
  - certSIGN provides its services in accordance with its Certificate Policies and Certification Practice Statements,
- (3) maintained effective controls to provide reasonable assurance that:
- the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by certSIGN and its subcontractor); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- (4) maintained effective controls to provide reasonable assurance that:
- logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2.](#)

certSIGN does not escrow subscriber's keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

### **Certification authority's responsibilities**

certSIGN's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2.](#)

The following incidents were reported to Mozilla during the audit period and during the onsite inspection:

- certSIGN: Ransomware attack incident (Bugzilla 1859748) <sup>1</sup>
- certSIGN: Certificates with incorrect Subject attribute order ([https://bugzilla.mozilla.org/show\\_bug.cgi?id=1886624](https://bugzilla.mozilla.org/show_bug.cgi?id=1886624))<sup>2</sup>

---

<sup>1</sup> certSIGN notified the Qualified Auditor about the incident on 23.10.2023. The Qualified Auditor followed the management of this incident until it was successfully resolved.

- certSIGN: Delayed response to CPR ([https://bugzilla.mozilla.org/show\\_bug.cgi?id=1886626](https://bugzilla.mozilla.org/show_bug.cgi?id=1886626))<sup>2</sup>
- certSIGN: Delayed revocation ([https://bugzilla.mozilla.org/show\\_bug.cgi?id=1886627](https://bugzilla.mozilla.org/show_bug.cgi?id=1886627))<sup>2</sup>

certSIGN managed all incidents properly and no incident had effect to the security of the CA and Root CA systems.

### **Our independence and quality control**

We have complied with the independence and other ethical requirements of the [Code of Ethics for Professional Accountants](#) issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

### **Auditor's responsibilities**

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of certSIGN's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
- (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The Audit Team consisted of 5 persons including Audit Quality Reviewers. The team qualifications included CPA, PhD, CISA, CISM, CISSP and was led by Péter Máté Erdósi PhD CISA. The average years of auditing experience – auditing trust services or similar information systems – are 16 years in the audit team.

All team members have knowledge of

- (1) audit principles, practices and techniques,
- (2) the issues related to various areas of public key infrastructure of CAs information security including risk assessment/management, network security and physical security;
- (3) the applicable standards, publicly available specifications and regulatory requirements for CAs and other relevant publicly available specifications including standards for IT product evaluation; and
- (4) the WebTrust Audit processes.

Additional qualification and personal experience of the Lead Auditor, the Lead Auditor

- (1) has acted as auditor more than 35 complete trust service provider audits since 2000,

---

<sup>2</sup> This incident was reported to Mozilla during the onsite inspection. The Qualified Auditor followed the reporting events but this incident will be reported in the next Webtrust Audit Report because it happened out of the audit period.

- (2) has adequate knowledge and attributes to manage the audit process, and
- (3) has the competence to communicate effectively, both orally and in writing.

### Relative effectiveness of controls

The relative effectiveness and significance of specific controls at certSIGN and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

### Inherent limitations

Because of the nature and inherent limitations of controls, certSIGN's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

### Opinion

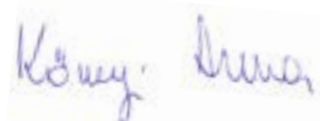
In our opinion, throughout the period 2023-02-08 to 2024-02-07, certSIGN management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

This report does not include any representation as to the quality of certSIGN's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), nor the suitability of any of certSIGN's services for any customer's intended purpose.

### Use of the WebTrust seal

certSIGN's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Crowe FST Audit Ltd.



Anna Kőszegi  
Partner



Dr. Péter Máté Erdősi, PhD CISA  
Director

**Annex**

<b>Root CA</b>	
<b>Subject</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	200605167002
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048 bit
<b>Digest Algorithm</b>	SHA1
<b>Not Before</b>	2006-07-04 17:20:04 GMT
<b>Not After</b>	2031-07-04 17:20:04 GMT
<b>SKI</b>	E08C9BDB2549B3F17C86D6B242870BD06BA0D9E4
<b>SHA256 Fingerprint</b>	EAA962C4FA4A6BAFEBE415196D351CCD888D4F53F3FA8AE6D7C466A94E6042BB

**Technically not constrained CAs**

<b>certSIGN SSL DV CA Class 3 G2</b>	
<b>Subject</b>	CN=certSIGN SSL DV CA Class 3 G2 OU=certSIGN SSL DV CA Class 3 G2 O=certSIGN C=RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	20060516700317887A0BE0D34AC3AF
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048 bit
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2018-01-30 09:44:44 GMT
<b>Not After</b>	2028-01-30 09:44:44 GMT
<b>SKI</b>	F5DCBBFB891ECA7881746CB64A6C254D54817E06
<b>SHA256 Fingerprint</b>	EA9A43515E138FF7782FCACDB9C7E8E1A61CFD1D17096ED5DDD1F400D02B03F5

<b>certSIGN Enterprise CA Class 3 G2</b>	
<b>Subject</b>	CN = certSIGN Enterprise CA Class 3 G2 OU = certSIGN Enterprise CA Class 3 G2 O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	2006051670030D545DC8613CF71AC5
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048 bit
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-04-29 13:14:30 GMT
<b>Not After</b>	2025-04-29 13:14:30 GMT
<b>SKI</b>	F6EB989E4069AB48609D4616FF9EC03B03BA9BFD
<b>SHA256 Fingerprint</b>	3B27DF9DD93C112AA08B062A6AE3973F7E79A5191D7E9B95D7081780E0D6ACEA

<b>certSIGN SSL EV CA Class 3 G2 – revoked on 2023-10-12</b>	
<b>Subject</b>	CN = certSIGN SSL EV CA Class 3 G2 OU = certSIGN SSL EV CA Class 3 G2 O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	200605167003185792601ACB75E127
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048 bit
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2018-01-30 09:46:55 GMT
<b>Not After</b>	2028-01-30 09:46:55 GMT
<b>SKI</b>	363BA29E25872A0FFD9A4A3C27DACBA779C30C7F
<b>SHA256 Fingerprint</b>	7826DE1BE414E454CFCAE0D17B17FF0CAD12EE68CF487F357B38499E274B0171

<b>certSIGN CA Class 2 G2</b>	
<b>Subject</b>	CN = certSIGN CA Class 2 G2 OU = certSIGN CA Class 2 G2 O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	20060516700310EF3C9EC6DC4CF90D
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-06-10 13:33:53 GMT
<b>Not After</b>	2025-06-10 13:33:53 GMT
<b>SKI</b>	45445b0621aa28088629ae09cf9d427f52427b19
<b>SHA256 Fingerprint</b>	35C0B8A577D11C94BA665E242DE45D6687522A531E391BB4D995D261F3829AB7

<b>certSIGN Non-Repudiation CA Class 4 G2</b>	
<b>Subject</b>	CN = certSIGN Non-Repudiation CA Class 4 G2 OU = certSIGN Non-Repudiation CA Class 4 G2 O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	2006051670031243F76E5DA85EACF3
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-06-10 13:54:42 GMT
<b>Not After</b>	2025-06-10 13:54:42 GMT
<b>SKI</b>	3FC1349B39F665DE86317DAB35E8197395DEF055
<b>SHA256 Fingerprint</b>	3003BF8853427C7B91023F7539853D987C58DC4E11BBE047D2A9305C01A6152C

<b>certSIGN Qualified CA Class 3 G2</b>	
<b>Subject</b>	CN = certSIGN Qualified CA Class 3 G2 OU = certSIGN Qualified CA Class 3 G2 O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	20060516700311549ACD829C4724B7
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-06-10 13:45:07 GMT
<b>Not After</b>	2025-06-10 13:45:07 GMT
<b>SKI</b>	50349E5376B96DD2B70C1E9083755AE ECB74188A
<b>SHA256 Fingerprint</b>	C89C24B415A72C9409667E88FB5E6E92A38D5609C3C99E55D99B4B1D458990F9

<b>CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3</b>	
<b>Subject</b>	CN = CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3 OU = Certificat de productie Production certificate O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	200605167003138995FB4FBF858BCF
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-09-10 12:32:18 GMT
<b>Not After</b>	2025-09-10 12:32:18 GMT
<b>SKI</b>	A9074811B8B295A0D572F12F552B987CEC2D299E
<b>SHA256 Fingerprint</b>	AA53452D589069EBD91423834FEC288A78ACC6A7B9D4D0F143D8C92E0B83D8E9

<b>CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3</b>	
<b>Subject</b>	CN = CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3 OU = Certificat de productie Production certificate O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	20060516700314CCB6A74F43ECDF8D
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-09-10 12:48:24 GMT
<b>Not After</b>	2025-09-10 12:48:24 GMT
<b>SKI</b>	20211332CA65A94A5B65F8414E1DE3FBB55B7F60
<b>SHA256 Fingerprint</b>	CAE72F66D61AFB9A697338E8F5358D8071BAFA4AE4D2717C7E635FB5EA43D365

<b>CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3</b>	
<b>Subject</b>	CN = CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3 OU = Certificat de test Test certificate O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	2006051670030EF4D27653C701A20B
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-04-29 14:33:36 GMT
<b>Not After</b>	2025-04-29 14:33:36 GMT
<b>SKI</b>	40C4001E2533BD69605E21DBD8843DE40EC5C6B8
<b>SHA256 Fingerprint</b>	01379EB7B85F68EDC2465B42438097687EBE1EAE49319639BFB342EFC3CEFA1D

<b>CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3</b>	
<b>Subject</b>	CN = CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3 OU = Certificat de test Test certificate O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	2006051670030F08BD2E1E01A473C7
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2015-04-29 14:45:24 GMT
<b>Not After</b>	2025-04-29 14:45:24 GMT
<b>SKI</b>	5778BB1E39FC276CA611165F52FA860A8F3F0263
<b>SHA256 Fingerprint</b>	0AC2B6086EB10DB5576A3A1B8EB0E4344082C1B7D832504FCBF95A4804D51834

<b>certSIGN Code Signing CA Class 3 G2 – revoked on 2023-10-12</b>	
<b>Subject</b>	CN = certSIGN Code Signing CA Class 3 G2 OU = certSIGN Code Signing CA Class 3 G2 O = certSIGN C = RO
<b>Issuer</b>	OU = certSIGN ROOT CA O = certSIGN C = RO
<b>Serial</b>	20060516700315A511AE66B97EF915
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2016-01-26 13:08:08 GMT
<b>Not After</b>	2026-01-26 13:08:08 GMT
<b>SKI</b>	BBA64E766BAA847013C2A7E868471D68C37E3E6F
<b>SHA256 Fingerprint</b>	785854130B14F6F1EE9F984257ABABB6255B05A8DBEFB7680D33400AC28FE909

30 April 2024

CERTSIGN S.A.  
MANAGEMENT'S ASSERTION

CERTSIGN Certification Authority ("certSIGN") is operated by CERTSIGN S.A. provides the following CA services under the Root CA with OU = certSIGN ROOT CA, O = certSIGN, C = RO, and 9 intermediate CA servers:

- Subscriber registration
- Certificate issuance
- Certificate distribution
- Certificate validation
- Certificate renewal
- Certificate revocation
- Subscriber key generation and management (except in case of SSL certificates)

The management of certSIGN is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure (<https://www.certsign.ro/en/repository/>) on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and intermediate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to certSIGN Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

certSIGN management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in providing its Certification Authority (CA) services at Bucharest, Romania, throughout the period 2023-02-08 to 2024-02-07, certSIGN has:

(1) disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the following documents:

- [Certification Policy, certSIGN, Version 1.14 as of 31 January 2023,](#)
- [Certification Policy, certSIGN, Version 1.15 as of 31 July 2023,](#)
- [Certification Policy, certSIGN, Version 1.16 as of 31 January 2024,](#)
- [Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.39 as of 31 January 2023,](#)
- [Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.40 as of 31 July 2023,](#)
- [Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.41 as of 31 January 2024,](#)
- [Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.40, Date: 31 July 2023,](#)

**certSIGN S.A.**VAT Code: **RO18288250**, Trade Register: **J40/484/2006**, Registered Capital: **2,095,560 LEI**Registered Office: 107A Dăbâncului Avenue, C1 Building, 1<sup>st</sup> Floor, Rooms 15, 54, Bucharest, RomaniaTelephone: +40 311011870, Fax: +40 21 311 99 05, E-mail: [office@certsign.ro](mailto: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-65030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-650322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

- [Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.41, Date: 31 August 2023,](#)
  - [Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.41a, Date: 31 January 2024,](#)
  - [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.16 as of 31 January 2023,](#)
  - [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.17 as of 15 May 2023,](#)
  - [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.18 as of 31 July 2023,](#)
  - [Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19 as of 31 January 2024,](#)
  - [Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.18, Date: 31 July 2023,](#)
  - [Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19, Date: 31 January 2024,](#)
  - Certification Practice Statement, certSIGN, SSL EV CA Class 3 G2 for SSL EV Certificates, Version 1.16 as of 31 January 2023 (retired),
  - Certification Practice Statement, certSIGN, SSL EV CA Class 3 G2 for SSL EV Certificates, Version 1.17 as of 31 July 2023 (retired on 2023-10-12)
- (2) maintained effective controls to provide reasonable assurance that:
- certSIGN Certification Practice Statements are consistent with its Certificate Policies
  - certSIGN provides its services in accordance with its Certificate Policies and Certification Practice Statements,
- (3) maintained effective controls to provide reasonable assurance that:
- the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by certSIGN and the external RA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- (4) maintained effective controls to provide reasonable assurance that:
- logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), including the following:

#### **CA Business Practices Disclosure**

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

#### **CA Business Practices Management**

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

#### **CA Environmental Controls**

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

#### **CA Key Lifecycle Management Controls**

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

#### **Subscriber Key Lifecycle Management Controls**

- Requirements for Subscriber Key Management

#### **Certificate Lifecycle Management Controls**

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

#### **certSIGN S.A.**

VAT Code: **RO18288250**, Trade Register: **J40/484/2006**, Registered Capital: **2,095,560 LEI**  
Registered Office: 107A Dilejtei Avenue, C1 Building, 1<sup>st</sup> Floor, Room 15, 54, Bucharest, Romania  
Telephone: +40 311011870, 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-65030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-650322: ICNET ISO 20000-1-ITSMS-31/13: ACCREDIA

certSIGN does not provide subscriber key escrow services, does not provide subscriber key generation services, and does not provide certificate suspension services.



Adrian Floarea  
CEO  
certSIGN S.A.

**certSIGN S.A.**

VAT Code: **RO18288250**, Trade Register: **J40/484/2006**, Registered Capital: **2,095,560 LEI**

Registered Office: 107A Oltenitei Avenue, C1 Building, 1<sup>st</sup> Floor, Room 15, 54, Bucharest, Romania

Telephone: +40 311011870, Fax: +40 21 311 99 05, E-mail: [office@certsign.ro](mailto: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