Crowe FST Audit Kft.
Member of Crowe Global

H-1124 Budapest
Jagelló út 14.
Hungary
Tel: +36 1 225-3490
Fax: +36 1 225-3491
www.crowe.hu

INDEPENDENT ASSURANCE REPORT

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

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 and Constanta, Romania, throughout the period 2024-02-08 to 2025-02-07 for its CAs as enumerated in **Annex A**, certSIGN has:

(1) disclosed its SSL certificate lifecycle management business practices in its:

- Certification Policy, certSIGN, Version 1.16 as of 31 January 2024,
- Certification Policy, certSIGN, Version 1.17 as of 18 April 2024,
- Certification Policy, certSIGN, Version 1.18 as of 15 January 2025,
- Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.41 as of 31 January 2024,
- Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.42 as of 18 April 2024,
- Certification Practice Statement, certSIGN ROOT CA & Intermediate CAs, Version 1.43 as of 15 January 2025,
- Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.41a, Date: 31 January 2024,
- Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.42, Date: 18 April 2024,
- Annex Profiles for Certification Practice Statement certSIGN ROOT CA & Intermediate CAs, Version 1.43, Date: 15 January 2025,
- Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19 as of 31 January 2024,
- Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.20 as of 15 January 2025,
- Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19, Date: 31 January 2024,
- Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.20, Date: 15 January 2025,

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the certSIGN website, and provided such services in accordance with its disclosed practices,

(2) maintained effective controls to provide reasonable assurance that:

- the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles;
- SSL 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

(3) 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

And, for its CAs as enumerated in **Annex A**:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, v2.7.

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

Certification authority's responsibilities

certSIGN 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 – SSL Baseline with Network Security, v2.7.

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

- certSIGN: Certificates with incorrect Subject attribute order (https://bugzilla.mozilla.org/show_bug.cgi?id=1886624)
- certSIGN: Delayed response to CPR (https://bugzilla.mozilla.org/show_bug.cgi?id=1886626)
- certSIGN: Delayed revocation (https://bugzilla.mozilla.org/show_bug.cgi?id=1886627)

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

Our independence and quality management

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 Management (ISQM) 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements 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.

Practitioner'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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, [and] obtaining an understanding of certSIGN's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 Erdősi PhD CISA. The average years of auditing experience – auditing trust services or similar information systems – are 17 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,

(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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period 2024-02-08 to 2025-02-07, 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 – SSL Baseline with Network Security, v2.7.

This report does not include any representation as to the quality of certSIGN services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, v2.7, nor the suitability of any of certSIGN services for any customer's intended purpose.

Use of the WebTrust seal

certSIGN's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security 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.
Budapest, Hungary

2025-04-30

Anna Kőszegi
Partner

Péter Máté Erdősi, PhD CISA
Director

Annex A

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

Technically not constrained living CAs

certSIGN certSIGN Web CA	
Subject	organizationIdentifier=VATRO-18288250, CN=certSIGN Web CA, O=CERTSIGN SA, C=RO
Issuer	OU=certSIGN ROOT CA, O=certSIGN, C=RO
Serial	2006051670031B56A93FC6CF742F9A
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	sha256
Not Before	2024-04-18 09:02:01 GMT
Not After	2026-04-18 09:02:01 GMT
SKI	65292B192B5A41D301629B7B4700E2180871C341
SHA256 Fingerprint	5D4494B65D1C14EF9959C539EABE21959F1A4A6880F13FDDB190B8B2E185CCDC

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

CAs for legacy purposes

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

certSIGN SSL EV CA Class 3 G2 – revoked on 2023-10-12	
Subject	CN = certSIGN SSL EV CA Class 3 G2 OU = certSIGN SSL EV CA Class 3 G2 O = certSIGN C = RO
Issuer	OU = certSIGN ROOT CA O = certSIGN C = RO
Serial	2006051670031857926O1ACB75E127
Key Algorithm	RSA
Key Size	2048 bit
Digest Algorithm	SHA256
Not Before	2018-01-30 09:46:55 GMT
Not After	2028-01-30 09:46:55 GMT
SKI	363BA29E25872A0FFD9A4A3C27DACBA779C30C7F
SHA256 Fingerprint	7826DE1BE414E454CFCAE0D17B17FF0CAD12EE68CF487F357B38499E274B0171

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

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

certSIGN Qualified CA Class 3 G2 – expires on 2025-06-10	
Subject	CN = certSIGN Qualified CA Class 3 G2 OU = certSIGN Qualified CA Class 3 G2 O = certSIGN C = RO
Issuer	OU = certSIGN ROOT CA O = certSIGN C = RO
Serial	20060516700311549ACD829C4724B7
Key Algorithm	RSA
Key Size	2048
Digest Algorithm	SHA256
Not Before	2015-06-10 13:45:07 GMT
Not After	2025-06-10 13:45:07 GMT
SKI	50349E5376B96DD2B70C1E9083755AEECB74188A
SHA256 Fingerprint	C89C24B415A72C9409667E88FB5E6E92A38D5609C3C99E55D99B4B1D458990F9

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

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

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

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

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

certSIGN S.A.
MANAGEMENT'S ASSERTION

certSIGN S.A. ("certSIGN") operates CERTSIGN Certification Authority (CA) services known as

- certSIGN Root CA (https://crt.sh/?caid=247)
- certSIGN Web CA (https://crt.sh/?caid=80378)
- certSIGN SSL DV CA Class 3 G2 (https://crt.sh/?caid=71635)
- CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3 (https://crt.sh/?caid=6774)
- CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3 (https://crt.sh/?caid=34344)
- CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3 (https://crt.sh/?caid=34347)
- CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3 (https://crt.sh/?caid=34345)
- certSIGN CA Class 2 G2 (https://crt.sh/?caid=12220)
- certSIGN Code Signing CA Class 3 G2 (https://crt.sh/?caid=34350)
- certSIGN Non-Repudiation CA Class 4 G2 (https://crt.sh/?caid=12530)
- certSIGN Qualified CA Class 3 G2 (https://crt.sh/?caid=6736)
- certSIGN SSL EV CA Class 3 G2 (https://crt.sh/?caid=71636)

and provides SSL CA services.

The management of certSIGN is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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's 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 SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Bucharest and Constanta, Romania throughout the period 2024-02-08 to 2025-02-07, certSIGN has:

(1) disclosed its SSL certificate lifecycle management business practices in its:

- Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19 as of 31 January 2024,
- Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.20 as of 15 January 2025,
- Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.19, Date: 31 January 2024,
- Annex Profiles for Certification Practice Statement, certSIGN, SSL DV CA Class 3 G2 for SSL DV certificates, Version 1.20, Date: 15 January 2025,

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the certSIGN website, and provided such services in accordance with its disclosed practices,

(2) maintained effective controls to provide reasonable assurance that:

- the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles;
- SSL subscriber information is properly authenticated (for the registration activities performed by certSIGN and the subcontractor);

(3) 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

(4) maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, version 2.7.

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.
Bucharest, 2024-04-30