

Management's Assertion Regarding the Effectiveness of Its Controls Over the Certification Authority Operations Based on the Trust Services Principles and Criteria for Certification Authorities Version 2.2

April 30, 2020

We, as management of S.C. certSIGN S.A., are responsible for operating a Certification Authority (CA) at Bvl. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, Bucharest, Romania, CP 050881, Romania for the Root CA and Subordinate CAs listed in Appendix A.

S.C. certSIGN S.A.'s CA services provide the following certification authority services:

- **Subscriber registration**
- **Certificate renewal**
- **Certificate rekey**
- **Certificate issuance**
- **Certificate distribution**
- **Certificate revocation**
- **Certificate suspension**
- **Certificate validation**
- **Subordinate CA cross-certification**
- **Subscriber key generation and management**

Management of S.C. certSIGN S.A. is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website (Appendix B), CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to S.C. certSIGN S.A.'s CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of S.C. certSIGN S.A. has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in S.C. certSIGN S.A. Management's opinion, in providing its CA services for the Root CA and Subordinate CAs listed in Appendix A at Bvl. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, Bucharest, Romania, CP 050881, Romania locations during the period from February 08, 2019 through February 07, 2020, S.C. certSIGN S.A. has:

- Disclosed its Business, Key Life Cycle Management, and Certificate Life Cycle Management, and CA Environmental Control practices as below:
 - certSIGN ROOT CA
 - certSIGN CA Class 2 G2
 - certSIGN Qualified CA Class 3 G2
 - certSIGN Enterprise CA Class 3 G2

- certSIGN Code Signing CA Class 3 G2
 - certSIGN SSL DV CA Class 3 G2
 - certSIGN SSL EV CA Class 3 G2
 - certSIGN Non-Repudiation CA Class 4 G2
 - CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3
 - CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3
 - CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3
 - CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3
- Maintained effective controls to provide reasonable assurance that:
 - S.C. certSIGN S.A. - CA's Certification Practice Statements (Appendix B No.2 and No.3) is consistent with its Certificate Policy (Appendix B No.1)
 - S.C. certSIGN S.A. - CA provides its services in accordance with its Certificate Policy and Certification Practice Statements (Appendix B No.2 and No.3)
 - Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - The integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
 - The Subscriber information was properly authenticated (for the registration activities performed by S.C. certSIGN S.A.); and
 - Subordinate CA certificate requests were accurate, authenticated and approved
 - Maintained effective controls to provide reasonable assurance that:
 - Logical and physical access to CA systems and data was restricted to authorized individuals;
 - The continuity of key and certificate management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the Root Keys listed in Appendix A, based on the *Trust Services Principles and Criteria for Certification Authorities Version 2.2*, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS) (Appendix B No.2 and No.3)
- Certificate Policy (CP) (Appendix B No.1)

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
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Very truly yours,

S.C. certSIGN S.A.

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA 256 fingerprint
C=RO, O=certSIGN, OU=certSIGN ROOT CA	E0:8C:9B:DB:25:49:B3:F 1:7C:86:D6:B2:42:87:0B: D0:6B:A0:D9:E4	35210227249154 (0x200605167002)	EAA962C4FA4A6BAFEBE415 196D351CCD888D4F53F3FA 8AE6D7C466A94E6042BB
C=RO, O=certSIGN, OU=certSIGN CA Class 2 G2, CN=certSIGN CA Class 2 G2	45:44:5B:06:21:AA:28:08: 86:29:AE:09:CF:9D:42:7F :52:42:7B:19	20:06:05:16:70:03:10:ef: 3c:9e:c6:dc:4c:f9:0d	35C0B8A577D11C94BA665E 242DE45D6687522A531E391 BB4D995D261F3829AB7
C=RO, O=certSIGN, OU=certSIGN Qualified CA Class 3 G2, CN=certSIGN Qualified CA Class 3 G2	50:34:9E:53:76:B9:6D:D2 :B7:0C:1E:90:83:75:5A:E E:CB:74:18:8A	20:06:05:16:70:03:11:54 :9a:cd:82:9c:47:24:b7	C89C24B415A72C9409667E8 8FB5E6E92A38D5609C3C99 E55D99B4B1D458990F9
C=RO, O=certSIGN, OU=certSIGN Enterprise CA Class 3 G2, CN=certSIGN Enterprise CA Class 3 G2	F6:EB:98:9E:40:69:AB:48 :60:9D:46:16:FF:9E:C0:3 B:03:BA:9B:FD	20:06:05:16:70:03:0d:54 :5d:c8:61:3c:f7:1a:c5	3B27DF9DD93C112AA08B06 2A6AE3973F7E79A5191D7E9 B95D7081780E0D6ACEA
C=RO, O=certSIGN, OU=certSIGN Code Signing CA Class 3 G2, CN=certSIGN Code Signing CA Class 3 G2	BB:A6:4E:76:6B:AA:84:7 0:13:C2:A7:E8:68:47:1D: 68:C3:7E:3E:6F	20:06:05:16:70:03:15:a5 :11:ae:66:b9:7e:f9:15	785854130B14F6F1EE9F984 257ABABB6255B05A8DBEFB 7680D33400AC28FE909
C=RO, O=certSIGN, OU=certSIGN SSL DV CA Class 3 G2, CN=certSIGN SSL DV CA Class 3 G2	F5:DC:BB:FB:89:1E:CA:7 8:81:74:6C:B6:4A:6C:25: 4D:54:81:7E:06	20:06:05:16:70:03:17:88 :7a:0b:e0:d3:4a:c3:af	EA9A43515E138FF7782FCA CDB9C7E8E1A61CFD1D1709 6ED5DDD1F400D02B03F5
C=RO, O=certSIGN, OU=certSIGN SSL EV CA Class 3 G2, CN=certSIGN SSL EV CA Class 3 G2	36:3B:A2:9E:25:87:2A:0F :FD:9A:4A:3C:27:DA:CB: A7:79:C3:0C:7F	20:06:05:16:70:03:18:57 :92:60:1a:cb:75:e1:27	7826DE1BE414E454CFCAE0 D17B17FF0CAD12EE68CF48 7F357B38499E274B0171
C=RO, O=certSIGN, OU=certSIGN Non-Repudiation CA Class 4 G2, CN=certSIGN Non-Repudiation CA Class 4 G2	3F:C1:34:9B:39:F6:65:DE :86:31:7D:AB:35:E8:19:7 3:95:DE:F0:55	20:06:05:16:70:03:12:43 :f7:6e:5d:a8:5e:ac:f3	3003BF8853427C7B91023F7 539853D987C58DC4E11BBE 047D2A9305C01A6152C
C=RO, O=certSIGN, OU=Certificat de productie Production certificate, CN=CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3	20:21:13:32:CA:65:A9:4A :5B:65:F8:41:4E:1D:E3:F B:B5:5B:7F:60	20:06:05:16:70:03:14:cc: b6:a7:4f:43:ec:df:8d	CAE72F66D61AFB9A697338 E8F5358D8071BAFA4AE4D2 717C7E635FB5EA43D365
C=RO, O=certSIGN, OU=Certificat de test Test certificate, CN=CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3	57:78:BB:1E:39:FC:27:6C :A6:11:16:5F:52:FA:86:0A :8F:3F:02:63	20:06:05:16:70:03:0f:08: bd:2e:1e:01:a4:73:c7	0AC2B6086EB10DB5576A3A 1B8EB0E4344082C1B7D8325 04FCBF95A4804D51834
C=RO, O=certSIGN, OU=Certificat de productie Production certificate, CN=CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3	A9:07:48:11:B8:B2:95:A0: D5:72:F1:2F:55:2B:98:7C :EC:2D:29:9E	20:06:05:16:70:03:13:89 :95:fb:4f:bf:85:8b:cf	AA53452D589069EBD914238 34FEC288A78ACC6A7B9D4D 0F143D8C92E0B83D8E9
C=RO, O=certSIGN, OU=Certificat de test Test certificate, CN=CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3	40:C4:00:1E:25:33:BD:69 :60:5E:21:DB:D8:84:3D:E 4:0E:C5:C6:B8	20:06:05:16:70:03:0e:f4: d2:76:53:c7:01:a2:0b	01379EB7B85F68EDC2465B4 2438097687EBE1EAE493196 39BFB342EFC3CEFA1D

Appendix B

No.	The list of audited certificate practices and procedures	Document Links
1.	Certification Policy certSIGN Version 1.7 Date: 31 January, 2019	https://www.certsign.ro/media/document/bXBCT2FNWUR4b0ZrcDNjY09qYmRhdz09/original/CP_certSIGN_Law_v1.7_January_2019_rev_.pdf
2.	Certification Practice Statement Version 1.24 Date: 16 September, 2019	https://www.certsign.ro/media/document/VmczeXh4bIVZTEwyRVdsaE1mdGFLdz09/original/CPS_EN_Law_v1.24_September_2019.pdf
3.	Certification Practice Statement certSIGN SSL DV CA Class 3 G2 for SSL DV certificates Version 1.4 Date: 31 January, 2019	https://www.certsign.ro/media/document/NEZxZGh0RTdZUHdUUIFZYk1xdFZydz09/original/CPS%20DV-v%201.4%20Law_January%202019%20rev&underscore_.pdf