



KPMG Advisory N.V.
IT Assurance
P.O. Box 74500
1070 DB Amsterdam
The Netherlands

Laan van Langerhuize 1
1186 DS Amstelveen
The Netherlands
Telephone +31 (0)20 656 7890
www.kpmg.com/nl

To the management of Logius

Amstelveen, 25 March 2026

Subject: Independent Auditor's Report WebTrust for CAs

We have been engaged, in a reasonable assurance engagement, to report on Logius' management's assertion that for its Certification Authority (CA) operations in the Netherlands, throughout the period 1 January 2025 through 31 December 2025 for its CAs as enumerated in Attachment A (referred to collectively as the Central Infrastructure of the Dutch Government PKI "PKIoverheid"), Logius has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [Certificate Practice Statement, version 5.4, dated December 2024](#)
 - [Certificate Practice Statement, version 5.5, dated July 2025](#)
- maintained effective controls to provide reasonable assurance that:
 - Logius provides its services in accordance with its Certification Practice Statement.
- 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 of TSPs, as performed by Logius); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- 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 [Trust Services Principles and Criteria for Certification Authorities, version 2.2.2.](#)

Document classification:

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026

Logius provides certificates to Trust Service Providers ("TSPs") for subscriber registration activities, as disclosed in Logius' business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

Logius does not provide or support CA Key Escrow, CA-Provided Subscriber Key Generation Services, CA-Provided Subscriber Key Storage and Recovery Services, Integrated Circuit Card (ICC) Lifecycle Management, Certificate Renewal, Certificate Rekey and Certificate Suspension. Additionally, Logius does not perform Subscriber Registration other than the TSPs which act as subordinate CAs. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification Authority's responsibilities

Logius' 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.

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 behaviour. Therefore, we are independent of Logius and complied with other ethical requirements in accordance with the '*Reglement Gedragscode Register IT-Auditors*' (Code of Ethics) of NOREA.

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. We also apply the '*Reglement Kwaliteitsbeheersing NOREA*' (RKBN, Regulations for Quality management systems) and, accordingly, maintain 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 and the related Dutch Directive 3000A '*Attest-opdrachten*' (Attestation engagements), as issued by NOREA, the IT Auditors Association in The Netherlands.



*Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026*

These standards require 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 Logius' 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 relative effectiveness and significance of specific controls at Logius 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, 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 controls may become ineffective.

Opinion

In our opinion, throughout the period 1 January 2025 through 31 December 2025, Logius 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 Logius' services beyond those covered by the WebTrust® Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of Logius' services for any customer's intended purpose.



*Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026*

Use of the WebTrust seal

Logius' 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.

On behalf of KPMG Advisory N.V.
Amstelveen, 25 March 2026

Original signed by

drs. ing. R.F. Koorn RE CISA
Partner



Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026

Attachment A: List of CAs in scope

The following CAs were in scope of the WebTrust for CAs Audit:

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
1	CN = Staat der Nederlanden Root CA – G3 O = Staat der Nederlanden C = NL	Self-signed	98a239	RSA	4096 bits	sha256RSA	14 November 2013	13 November 2028	54adfacc79257aec a359c2e12f4e4b a5d20dc9457	3C4FB0B95AB8B30032F432 B86F535FE172C185D0FD39 865837CF36187FA6F428	
2	CN = Staat der Nederlanden – G4 Root Publ G-SMIME – 2024 O = Staat der Nederlanden C = NL	Self-signed	1a:9f:45:e4: 69:54:1e:92 :73:18:31:9 a:ee:dd:b4: 7b:1b:84:3a :2e	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2039	9bf8804e32827e 7125c96ebf240e 59aa447048c9	B80BF76624198A2D5D2820 68B49EF370AD901AB3A428 97B628EFE6E6980B0A4E	
3	CN = Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024 O = Staat der Nederlanden C = NL	Self-signed	3b:d6:ec:92 :d9:0b:c1:df :5e:3c:60:c c:7d:ef:dd:3 1:96:f6:b0:4 e	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	262ef8e7f5c977a b038b7b7efa4c1 47331c8796c	5C8CAE4CDBC0DE389310D E0FE5A9A52133B74C2D20A 806689417AE6682979474	
4	CN = Staat der Nederlanden - G4 Root Priv G-Other - 2024 O = Staat der Nederlanden C = NL	Self-signed	29:00:23:ff: 7f:de:8a:02: b1:42:06:ad :b1:45:b8:1 8:2f:c9:b7:4 6	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	79ebc108d1e062 8eea4ea7c6b9fb 9351e89f9926	9292375818F35F2611632DC 7056FA72A715021BC5610C 8B505B570E732EFCE81	
5	CN = Staat der Nederlanden - G4 Root Priv G-TLS - 2024 O = Staat der Nederlanden C = NL	Self-signed	08:94:0d:d3 :61:c3:98:4 a:65:6c:59: 3d:04:1e:c1 :1f:3f:16:48: c4	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	6eec08fe83ad14 2dadb4b6345113 9771225e4ea9	4411F67D3D7F4F49D34FF8 862249DE0D6692ADC92DF 0855FB1DD67A169800484	
6	CN = Staat der Nederlanden - G4 Root Priv S-CIBG - 2024 O = Staat der Nederlanden C = NL	Self-signed	3b:68:47:03 :eb:c0:24:a 3:29:3f:ca:b 7:26:8d:3a: 1a:31:f7:f6: 26	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	515c95b6abcbbc d34315a363e9ea 16cf5f375b5d	CA54D3B8B32A8A1ECE9E0 BB5DEC603F982A8FB8D69 3F9B2EBC22297FE7059BFD	

Document classification:

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



*Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026*

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
7	CN = Staat der Nederlanden Burger CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a247	RSA	4096 bits	sha256RSA	14 November 2013	12 November 2028	ff6875427dfa6fc7 5a93389f3544d0 aa2d00b289	2E7A0A3B0C527EB20C5225 3C8D2278CA108136A8CA3 A4EA22DA7B59BAC90650A	
8	CN = Staat der Nederlanden Organisatie Services CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a23c	RSA	4096 bits	sha256RSA	14 November 2013	12 November 2028	43eb4d00d39593 cea67c400d6d11 be39d132aee2	D9581DBDE99B39EEFF6CE 5C80DE1650DA0C1C8A109 705ED286C53BC95E6655E4	
9	CN = Staat der Nederlanden Organisatie Persoon CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a246	RSA	4096 bits	sha256RSA	14 November 2013	12 November 2028	eeac6d40ead504 6a872c557bf53f2 ddaeeadbace2	8222BC4FE7A3DDCA9EF0B F0D682AC888799F87822D1 5332A54C0BFD6C6854F7B	
10	CN = Staat der Nederlanden Autonome Apparaten CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a2a0	RSA	4096 bits	sha256RSA	15 November 2013	12 November 2028	6d1b25025de048 f46e1375e25784 9d50f3301443	AD493D6E85EC608AB813A 887BDC4D4196A0BC9B33D 2565A7FA8AC430F08A99A5	
11	CN = Staat der Nederlanden Organization Services CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	55:ad:e7:48 :06:18:27:e 8:b9:28:8b: 3c:4e:33:58 :39:50:93:9 a:e8	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	18f877cd90ef529 f5a7c3f51be1208 ab8e4f093f	5352C1F494BCAC98E69C9 C85D3D0418F7CED8C0487 4FD3C9FE7DBEBE7ADBE7 3D	
12	CN = Staat der Nederlanden Citizen CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	35:2e:f9:fd: 94:ba:19:64 :4e:a2:9a:4 2:e4:a8:93: 1e:ef:b3:fb: da	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	9968db4e823d34 becf87eb274192 7a4e3d9da847	A67A56A183EDE6EB89CB8 5A85BCD52CE1EF925251A A239AD25616C12C8088C06	
13	CN = Staat der Nederlanden Organization Person CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	1C:22:5B:9 E:D2:83:C C:21:B6:FE :6B:27:20:A D:90:42:2B: 4D:47:A4	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	257906c6a631fd df9e71a0fe4b313 71710ee46bc	BF45E3CE00CF22B8FC505 BCA3875C6C85BC4FF5F2D 9B439180829963307D8DC9	

Document classification:

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
14	CN = Staat der Nederlanden S/MIME CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	63:00:fd:22: 22:7d:9c:7c :2f:43:66:b5 :cf:80:e5:2f: 85:e4:3e:f7	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	533cb869889605 0a41739329cb22 e2accd1e2160	F0305F07AB78862F2F11E4 DEFE6E5EB749F8686B5461 3355A4845DE2052C73DE	
15	CN = Staat der Nederlanden - G4 Intm EUTL G-Sigs LP - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024	23:4a:08:f9: d1:30:2f:c4: 51:16:88:2e :98:a0:e1:7 9:52:f4:b6:7 2	RSA	4096 bits	sha512	30 May 2024	19 May 2039	1e31e89a1a1fcf f7f5386f47d057c 26a89c2835	EA5D15B9802CB3E29D566 A00AF51A7E7B829E75D67C B2D908392C347B2F3C174	
16	CN = Staat der Nederlanden - G4 Intm EUTL G-Sigs NP - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024	6a:6b:b0:9e :d0:d7:d8:6 b:31:03:95: c0:d3:bd:3a :eb:f3:c7:36 :86	RSA	4096 bits	sha512	30 May 2024	19 May 2039	6600b18fe014b8 76b6dd04fd7f611 dff4a634d70	76A62072D1DE085F5007C8 C15B51D2F34BD279ED57F 84CC26142C03E0B95F75C	
17	CN = Staat der Nederlanden - G4 Intm Priv G-Other NP - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root Priv G-Other - 2024	2e:38:2d:9c :a5:c7:49:1f :a9:30:19:b 0:92:63:4c: 72:e9:ef:c8: 57	RSA	4096 bits	sha512	30 May 2024	19 May 2039	5f2452ca005766 2eaaadb2d23799 3a04c271c0cb	487143968D1F7D70C707A6 62F1F8F045783C7522DB74 3988FB398D4DD78D6E75	
18	CN = Staat der Nederlanden - G4 Intm Priv G-Other LP - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root Priv G-Other - 2024	10:f2:90:82: 17:a6:96:cd :d0:69:7e:cf :91:8d:7b:3 1:82:54:9b: 3f	RSA	4096 bits	sha512	30 May 2024	19 May 2039	d589a50b81ff2e1 06856410719198 d23996829f6	FED07CE4B00D5436DDEFA 0D7C20A45800DD8DA40DE A3B1079F232E50BE594C4F	
19	CN = Staat der Nederlanden - G4 Intm Priv G-TLS SYS - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root Priv G-TLS - 2024	55:17:38:b9 :07:42:c8:d 4:08:fd:e1:a 7:6d:c2:5f:0 7:35:07:52: d3	RSA	4096 bits	sha512	27 Jun 2024	19 May 2039	992edd37595134 adc8fec65da6e48 120dc0ffc83	A24F6F2FA192DD96CEEAF 8D4C380D8663426F958589 56A5ADFF5CFD36B30554F	

Document classification:

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



*Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026*

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
20	CN = Staat der Nederlanden - G4 Intm Priv S-CIBG NP - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root Priv S-CIBG - 2024	35:3c:61:b5:be:78:e3:86:f9:4a:14:e9:0a:82:ad:80:68:d6:7e:d7	RSA	4096 bits	sha512	27 Jun 2024	19 May 2039	20cb7262f7314a a74ea9fbf8600a8 cbad730e8ed	4BDE8352F73C9EBB5AB1E CD368AF96C7FF733B4CB7 27FA819C02BA2A5D5357A7	
21	CN = Staat der Nederlanden - G4 Intm Priv S-CIBG LP - 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden - G4 Root Priv S-CIBG - 2024	29:1e:63:db:82:f8:81:54:ff:e7:d5:6d:9a:96:bf:fb:bb:dc:84:77	RSA	4096 bits	sha512	27 Jun 2024	19 May 2039	a835e3b3ef7d33 45f2d18569444b d974c4d0bea6	94548E125D3F94B32A734B 81E416E703C52C3DBBF240 5FCED9DDC1F0806B0423	



*Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026*

Attachment B: Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Delayed S/MIME audit report for MoD PKIoverheid G3 CA	Bugzilla Ticket Link
2	TSP KPN Findings in 2025 ETSI Audit - Incident Report #1 – Security Handbook	Bugzilla Ticket Link
3	TSP KPN Findings in 2025 ETSI Audit - Incident Report #2 – Compliance Management	Bugzilla Ticket Link
4	TSP KPN Findings in 2025 ETSI Audit - Incident Report #3 – Internal Audit	Bugzilla Ticket Link
5	TSP KPN Findings in 2025 ETSI Audit - Incident Report #4 – Training	Bugzilla Ticket Link
6	TSP KPN Findings in 2025 ETSI Audit - Incident Report #5 – CMDB	Bugzilla Ticket Link
7	TSP KPN Findings in 2025 ETSI Audit - Incident Report #6 – Security Incident Procedure	Bugzilla Ticket Link
8	TSP KPN Findings in 2025 ETSI Audit - Incident Report #7 – Change Management	Bugzilla Ticket Link
9	TSP KPN Findings in 2025 ETSI Audit - Incident Report #8 – Logical Access	Bugzilla Ticket Link
10	TSP KPN Findings in 2025 ETSI Audit - Incident Report #9 – Lifecycle Management	Bugzilla Ticket Link
11	TSP KPN Findings in 2025 ETSI Audit - Incident Report #10 – Firewall Rules and Review	Bugzilla Ticket Link
12	TSP KPN Findings in 2025 ETSI Audit - Incident Report #11 – Anti-Malware Software	Bugzilla Ticket Link
13	TSP KPN Findings in 2025 ETSI Audit - Incident Report #12 – Outdated Software	Bugzilla Ticket Link
14	TSP KPN Findings in 2025 ETSI Audit - Incident Report #13 – Restore Test	Bugzilla Ticket Link
15	TSP KPN Findings in 2025 ETSI Audit - Incident Report #14 – Back-up	Bugzilla Ticket Link
16	TSP KPN Findings in 2025 ETSI Audit - Incident Report #15 – Outdated Software	Bugzilla Ticket Link
17	TSP KPN Findings in 2025 ETSI Audit - Incident Report #16 – EJBCA Configuration	Bugzilla Ticket Link
18	TSP Cleverbase Findings in 2025 ETSI Audit - Incident Report #1 – Incorrect issuer CA listed in CPS	Bugzilla Ticket Link
19	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #1 – Document Management	Bugzilla Ticket Link
20	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #2 – Supply Chain Management	Bugzilla Ticket Link
21	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #3 – Asset Management	Bugzilla Ticket Link
22	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #4 – Incident Management	Bugzilla Ticket Link
23	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #5 – Risk Management	Bugzilla Ticket Link
24	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #6 – Access Control Management	Bugzilla Ticket Link
25	TSP CIBG Findings in 2025 ETSI Audit - Incident Report #7 – Change Management	Bugzilla Ticket Link

Document classification:

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



*Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 25 March 2026*

#	Disclosure	Publicly Disclosed Link
26	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #8 – Human Resources Management	Bugzilla Ticket Link



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Management Assertion Logius WebTrust for CAs 2025

Date 21 March 2026

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from 1 January 2025 through 31 December 2025

LOGIUS MANAGEMENT'S ASSERTION

The Dutch Governmental Service Organisation for ICT "Logius" provides the following Certification Authority (CA) services known as "PKIoverheid" through the central infrastructure of the Dutch Government:

- Subscriber registration
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate validation (using an online repository)

Logius provides certificates to Trust Service Providers (TSPs) in order to become part of the Dutch Government PKI, named "PKIoverheid". The practices outlining the processes related to accession, supervision and control are described in the PKIoverheid Certification Practice Statement, as is published on the website of the Policy Authority PKIoverheid.

The management of Logius is responsible for the central infrastructure of the Dutch Government PKI and responsible for establishing and maintaining effective controls over its Certification Authority operations, including:

- CA business practices disclosure in its Certification Practice Statement on the website of the Policy Authority PKIoverheid;
- Service integrity, including key and certificate lifecycle management controls, and
- CA environmental 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 Logius' Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of Logius has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Logius management's opinion, in providing its Certification Authority (CA) services in the Netherlands, throughout the period 1 January 2025 to 31 December 2025 for its CAs as enumerated in Attachment A, Logius has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its:
 - Certificate Practice Statement, version 5.4, dated December 2024;
 - Certificate Practice Statement, version 5.5, dated July 2025.
- maintained effective controls to provide reasonable assurance that:
 - Logius provides its services in accordance with its Certification Practice Statement.

- 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;
 - the Subscriber information is properly authenticated (for the registration activities of TSP's as performed by Logius); and
 - subordinate CA certificate requests are accurate, authenticated, and approved.
- 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.

Based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy

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 and 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 Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Logius does not provide or support CA Key Escrow, CA-Provided Subscriber Key Generation Services, CA-Provided Subscriber Key Storage and Recovery Services, Integrated Circuit Card (ICC) Lifecycle Management, Certificate Renewal, Certificate Rekey and Certificate Suspension. Additionally, Logius does not perform Subscriber Registration other than the TSPs which act as subordinate CAs. Accordingly, our assertion does not extend to controls that would address those criteria.

On behalf of

The Secretary of State of Kingdom Relations and Effective Government,

Logius,

Original signed by

M. van Loon
Directeur Programmaregie, Stelsels & Standaarden a.i.

Attachment A: List of CAs in scope

The following CAs were in scope of the WebTrust for CA Audit:

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
1	CN = Staat der Nederlanden Root CA – G3 O = Staat der Nederlanden C = NL	Self-signed	98a239	RSA	4096 bits	sha256RSA	14 November 2013	13 November 2028	54adfacc79257aec a359c2e12fbeb4b a5d20dc9457	3C4FB0B95AB8B30032F432B 86F535FE172C185D0FD3986 5837CF36187FA6F428	
2	CN = Staat der Nederlanden – G4 Root Publ G-SMIME – 2024 O = Staat der Nederlanden C = NL	Self-signed	1a:9f:45:e4 :69:54:1e: 92:73:18:3 1:9a:ee:dd: b4:7b:1b:8 4:3a:2e	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2039	9bf8804e32827e 7125c96ebf240e 59aa447048c9	B80BF76624198A2D5D28206 8B49EF370AD901AB3A42897 B628EFE6E6980B0A4E	
3	CN = Staat der Nederlanden – G4 Root EUTL G-Sigs – 2024 O = Staat der Nederlanden C = NL	Self-signed	3b:d6:ec:9 2:d9:0b:c1: df:5e:3c:60 :cc:7d:ef:d d:31:96:f6: b0:4e	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	262ef8e7f5c977a b038b7b7efa4c1 47331c8796c	5C8CAE4CDBC0DE389310DE 0FE5A9A52133B74C2D20A80 6689417AE6682979474	
4	CN = Staat der Nederlanden – G4 Root Priv G-Other – 2024 O = Staat der Nederlanden C = NL	Self-signed	29:00:23:ff :7f:de:8a:0 2:b1:42:06 :ad:b1:45:b 8:18:2f:c9: b7:46	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	79ebc108d1e062 8eea4ea7c6b9fb 9351e89f9926	9292375818F35F2611632DC 7056FA72A715021BC5610C8 B505B570E732EFCE81	
5	CN = Staat der Nederlanden – G4 Root Priv G-TLS – 2024 O = Staat der Nederlanden C = NL	Self-signed	08:94:0d:d 3:61:c3:98: 4a:65:6c:5 9:3d:04:1e :c1:1f:3f:1 6:48:c4	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	6eec08fe83ad14 2dadb4b6345113 9771225e4ea9	4411F67D3D7F4F49D34FF88 62249DE0D6692ADC92DF08 55FB1DD67A169800484	
6	CN = Staat der Nederlanden – G4 Root Priv S-CIBG – 2024 O = Staat der Nederlanden C = NL	Self-signed	3b:68:47:0 3:eb:c0:24: a3:29:3f:ca :b7:26:8d: 3a:1a:31:f7 :f6:26	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2029	515c95b6abcbbc d34315a363e9ea 16cf5f375b5d	CA54D3B8B32A8A1ECE9E0B B5DEC603F982A8FB8D693F9 B2EBC22297FE7059BFD	

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
7	CN = Staat der Nederlanden Burger CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a247	RSA	4096 bits	sha256RSA	14 November 2013	12 November 2028	ff6875427dfa6fc75a93389f3544d0aa2d00b289	2E7A0A3B0C527EB20C52253C8D2278CA108136A8CA3A4EA22DA7B59BAC90650A	
8	CN = Staat der Nederlanden Organisatie Services CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a23c	RSA	4096 bits	sha256RSA	14 November 2013	12 November 2028	43eb4d00d39593cea67c400d6d11be39d132aee2	D9581DBDE99B39EEFF6CE5C80DE1650DA0C1C8A109705ED286C53BC95E6655E4	
9	CN = Staat der Nederlanden Organisatie Persoon CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a246	RSA	4096 bits	sha256RSA	14 November 2013	12 November 2028	eeac6d40ead5046a872c557bf53f2ddaee2	8222BC4FE7A3DDCA9EF0BF0D682AC888799F87822D15332A54C0BDFDC6854F7B	
10	CN = Staat der Nederlanden Autonome Apparaten CA – G3 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	98a2a0	RSA	4096 bits	sha256RSA	15 November 2013	12 November 2028	6d1b25025de048f46e1375e257849d50f3301443	AD493D6E85EC608AB813A887BDC4D4196A0BC9B33D2565A7FA8AC430F08A99A5	
11	CN = Staat der Nederlanden Organization Services CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	55:ad:e7:48:06:18:27:e8:b9:28:8b:3c:4e:33:58:39:50:93:9a:e8	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	18f877cd90ef529f5a7c3f51be1208ab8e4f093f	5352C1F494BCAC98E69C9C85D3D0418F7CED8C04874FD3C9FE7DBEBE7ADBE73D	
12	CN = Staat der Nederlanden Citizen CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	35:2e:f9:fd:94:ba:19:64:4e:a2:9a:42:e4:a8:93:1e:ef:b3:fb:da	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	9968db4e823d34becf87eb2741927a4e3d9da847	A67A56A183EDE6EB89CB85A85BCD52CE1EF925251AA239AD25616C12C8088C06	
13	CN = Staat der Nederlanden Organization Person CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	1C:22:5B:9E:D2:83:CC:21:B6:FE:6B:27:20:AD:90:42:2B:4D:47:A4	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	257906c6a631fd9f9e71a0fe4b31371710ee46bc	BF45E3CE00CF22B8FC505BCA3875C6C85BC4FF5F2D9B439180829963307D8DC9	

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
14	CN = Staat der Nederlanden S/MIME CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederlanden Root CA – G3	63:00:fd:22:22:7d:9c:7c:2f:43:66:b5:cf:80:e5:2f:85:e4:3e:f7	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	533cb8698896050a41739329cb22e2accd1e2160	F0305F07AB78862F2F11E4D EFE6E5EB749F8686B546133 55A4845DE2052C73DE	
15	CN = Staat der Nederlanden – G4 Intm EUTL G-Sigs LP – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root EUTL G-Sigs – 2024	23:4a:08:f9:d1:30:2f:c4:51:16:88:2e:98:a0:e1:79:52:f4:b6:72	RSA	4096 bits	sha512	30 May 2024	19 May 2039	1e31e89a1a1fcacf7f5386f47d057c26a89c2835	EA5D15B9802CB3E29D566A 00AF51A7E7B829E75D67CB2 D908392C347B2F3C174	
16	CN = Staat der Nederlanden – G4 Intm EUTL G-Sigs NP – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root EUTL G-Sigs – 2024	6a:6b:b0:9e:d0:d7:d8:6b:31:03:95:c0:d3:bd:3a:eb:f3:c7:36:86	RSA	4096 bits	sha512	30 May 2024	19 May 2039	6600b18fe014b876b6dd04fd7f611dff4a634d70	76A62072D1DE085F5007C8C 15B51D2F34BD279ED57F84C C26142C03E0B95F75C	
17	CN = Staat der Nederlanden – G4 Intm Priv G-Other NP – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root Priv G-Other – 2024	2e:38:2d:9c:a5:c7:49:1f:a9:30:19:b0:92:63:4c:72:e9:ef:c8:57	RSA	4096 bits	sha512	30 May 2024	19 May 2039	5f2452ca0057662eaaadb2d237993a04c271c0cb	487143968D1F7D70C707A66 2F1F8F045783C7522DB7439 88FB398D4DD78D6E75	
18	CN = Staat der Nederlanden – G4 Intm Priv G-Other LP – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root Priv G-Other – 2024	10:f2:90:82:17:a6:96:c:d:d0:69:7e:cf:91:8d:7b:31:82:54:9b:3f	RSA	4096 bits	sha512	30 May 2024	19 May 2039	d589a50b81ff2e106856410719198d23996829f6	FED07CE4B00D5436DDEFA0 D7C20A45800DD8DA40DEA3 B1079F232E50BE594C4F	
19	CN = Staat der Nederlanden – G4 Intm Priv G-TLS SYS – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root Priv G-TLS – 2024	55:17:38:b9:07:42:c8:d4:08:fd:e1:a7:6d:c2:5f:07:35:07:52:d3	RSA	4096 bits	sha512	27 Jun 2024	19 May 2039	992edd37595134adc8fec65da6e48120dc0ffc83	A24F6F2FA192DD96CEEAF8D 4C380D8663426F95858956A 5ADFF5CFD36B30554F	

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
20	CN = Staat der Nederlanden – G4 Intm Priv S-CIBG NP – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root Priv S-CIBG – 2024	35:3c:61:b5:be:78:e3:86:f9:4a:14:e9:0a:82:a:d:80:68:d6:7e:d7	RSA	4096 bits	sha512	27 Jun 2024	19 May 2039	20cb7262f7314a a74ea9fbf8600a8 cbad730e8ed	4BDE8352F73C9EBB5AB1EC D368AF96C7FF733B4CB727F A819C02BA2A5D5357A7	
21	CN = Staat der Nederlanden – G4 Intm Priv S-CIBG LP – 2024 O = Staat der Nederlanden C = NL	Staat der Nederlanden – G4 Root Priv S-CIBG – 2024	29:1e:63:db:82:f8:81:b:82:f8:81:54:ff:e7:d5:6d:9a:96:b:f:fb:bb:dc:84:77	RSA	4096 bits	sha512	27 Jun 2024	19 May 2039	a835e3b3ef7d33 45f2d18569444b d974c4d0bea6	94548E125D3F94B32A734B8 1E416E703C52C3DBBF2405F CED9DDC1F0806B0423	

Attachment B: Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Delayed S/MIME audit report for MoD PKIoverheid G3 CA	Bugzilla Ticket Link
2	TSP KPN Findings in 2025 ETSI Audit – Incident Report #1 – Security Handbook	Bugzilla Ticket Link
3	TSP KPN Findings in 2025 ETSI Audit – Incident Report #2 – Compliance Management	Bugzilla Ticket Link
4	TSP KPN Findings in 2025 ETSI Audit – Incident Report #3 – Internal Audit	Bugzilla Ticket Link
5	TSP KPN Findings in 2025 ETSI Audit – Incident Report #4 – Training	Bugzilla Ticket Link
6	TSP KPN Findings in 2025 ETSI Audit – Incident Report #5 – CMDB	Bugzilla Ticket Link
7	TSP KPN Findings in 2025 ETSI Audit – Incident Report #6 – Security Incident Procedure	Bugzilla Ticket Link
8	TSP KPN Findings in 2025 ETSI Audit – Incident Report #7 – Change Management	Bugzilla Ticket Link
9	TSP KPN Findings in 2025 ETSI Audit – Incident Report #8 – Logical Access	Bugzilla Ticket Link
10	TSP KPN Findings in 2025 ETSI Audit – Incident Report #9 – Lifecycle Management	Bugzilla Ticket Link
11	TSP KPN Findings in 2025 ETSI Audit – Incident Report #10 – Firewall Rules and Review	Bugzilla Ticket Link
12	TSP KPN Findings in 2025 ETSI Audit – Incident Report #11 – Anti-Malware Software	Bugzilla Ticket Link
13	TSP KPN Findings in 2025 ETSI Audit – Incident Report #12 – Outdated Software	Bugzilla Ticket Link
14	TSP KPN Findings in 2025 ETSI Audit – Incident Report #13 – Restore Test	Bugzilla Ticket Link
15	TSP KPN Findings in 2025 ETSI Audit – Incident Report #14 – Back-up	Bugzilla Ticket Link
16	TSP KPN Findings in 2025 ETSI Audit – Incident Report #15 – Outdated Software	Bugzilla Ticket Link
17	TSP KPN Findings in 2025 ETSI Audit – Incident Report #16 – EJBCA Configuration	Bugzilla Ticket Link
18	TSP Cleverbase Findings in 2025 ETSI Audit – Incident Report #1 – Incorrect issuer CA listed in CPS	Bugzilla Ticket Link
19	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #1 – Document Management	Bugzilla Ticket Link
20	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #2 – Supply Chain Management	Bugzilla Ticket Link
21	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #3 – Asset Management	Bugzilla Ticket Link
22	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #4 – Incident Management	Bugzilla Ticket Link
23	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #5 – Risk Management	Bugzilla Ticket Link
24	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #6 – Access Control Management	Bugzilla Ticket Link
25	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #7 – Change Management	Bugzilla Ticket Link
26	TSP CIBG Findings in 2025 ETSI Audit – Incident Report #8 – Human Resources Management	Bugzilla Ticket Link