



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 S/MIME Certificates

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 S/MIME certificate lifecycle management business practices in its:
 - [Certificate Practice Statement, version 5.4, dated December 2024](#)
 - [Certificate Practice Statement, version 5.5, dated July 2025](#)including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on Logius' website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities of TSP's, as performed by Logius); and
- 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 – S/MIME Certificates v1.0.8](#).

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities – Network Security address this requirement and are reported on in a separate report.

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 – S/MIME
Amstelveen, 25 March 2026

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 – S/MIME Certificates v1.0.8.

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.

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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates;
2. selectively testing transactions executed in accordance with disclosed S/MIME 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.



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

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 – S/MIME Certificates v1.0.8.

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 – S/MIME Certificates v1.0.8, nor the suitability of any of Logius' services for any customer's intended purpose.

Use of the WebTrust seal

Logius' use of the WebTrust for Certification Authorities – S/MIME Certificates 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 – S/MIME
Amstelveen, 25 March 2026

Attachment A: List of CAs in scope

The following CAs were in scope of the WebTrust for CAs S/MIME 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 a359c2e12fbc4b a5d20dc9457	3CAF0B95AB8B30032F432 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 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	2 ^F 7A0A3B0C527EB20C5225 3C8D2278CA108136A8CA3 A4EA22DA7B59BAC90650A	
4	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	
5	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 ddaeeedbase2	8222BC4FE7A3DDCA9EF0B F0D682AC888799F87822D1 5332A54C0BDFDC6854F7B	
6	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	
7	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 DEF6E5EB749F8686B5461 3355A4845DE2052C73DE	

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 – S/MIME
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

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 – S/MIME
Amstelveen, 25 March 2026*

#	Disclosure	Publicly Disclosed 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



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Management Assertion Logius
WebTrust for CAs – S/MIME 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 its S/MIME Certification Authority (CA) services known as "PKIoverheid" through the central infrastructure of the Dutch Government.

For the issuance of S/MIME CA services, the central infrastructure of the Dutch Government in 2025 consists of the following CAs:

- two Root CAs ("Staat der Nederlanden Root CA – G3", and "Staat der Nederlanden – G4 Root Publ G-SMIME - 2024")
- one intermediate CA ("Staat der Nederlanden S/MIME CA – 2023").

The other CAs listed in attachment A are included for various reasons:

- CAs 3,4 and 5 in attachment A were historically used to issue CA certificates to Trust Service Providers (TSPs) which in turn could issue working S/MIME certificates.
- The "Staat der Nederlanden Autonome Apparaten CA – G3" has only issued TSP certificates which are incapable for S/MIME but is technically unconstrained (no EKU in the intermediate CA).
- Since all of these intermediate CAs are either unconstrained or include the emailProtection Extended Key Usage (EKU) they are included in the processes and controls to which this management assertion applies, even if they never issued S/MIME certificates or have ceased issuance because they are Extant CAs per the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (SBRG) Appendix B and the period allowed for issuance for S/MIME certificates has expired. As such they do not contain the SBRG policy OIDs.

The management of Logius is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its network and certificate security system controls, its S/MIME CA business practices disclosure on its website, S/MIME key lifecycle management controls, and S/MIME 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 Logius' Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Logius' management has assessed its disclosures of its certificate practices and controls over its S/MIME CA services. Based on that assessment, in providing its S/MIME CA services in The Netherlands, throughout the period 1 January 2025 to 31 December 2025, Logius has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - Certificate Practice Statement, version 5.4, dated December 2024;
 - Certificate Practice Statement, version 5.5, dated July 2025

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

- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities performed by Logius)
- 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 – S/MIME Certificates v1.0.8.

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 S/MIME 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 a359c2e12f9e4b 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 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	ff6875427dfa6fc 75a93389f3544d 0aa2d00b289	2E7A0A3B0C527EB20C52253 C8D2278CA108136A8CA3A4 EA22DA7B59BAC90650A	
4	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	D9581DBDE99B39EEFF6CE5 C80DE1650DA0C1C8A10970 5ED286C53BC95E6655E4	
5	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 ddaeeedbase2	8222BC4FE7A3DDCA9EF0BF0 D682AC888799F87822D1533 2A54C0BDFDC6854F7B	
6	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	AD493D6E85EC608AB813A8 87BDC4D4196A0BC9B33D25 65A7FA8AC430F08A99A5	

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
7	CN = Staat der Nederlanden S/MIME CA – 2023 O = Staat der Nederlanden C = NL	Staat der Nederland en Root CA – G3	63:00:fd:22 :22:7d:9c:7 c:2f:43:66: b5:cf:80:e5 :2f:85:e4:3 e:f7	RSA	4096 bits	sha256RSA	31 October 2023	13 November 2028	533cb869889605 0a41739329cb22 e2accd1e2160	F0305F07AB78862F2F11E4D EFE6E5EB749F8686B546133 55A4845DE2052C73DE	

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

#	Disclosure	Publicly Disclosed 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