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, 27 March 2025

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 2024 through 31 December 2024 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 5.1, dated October 2023;
  - version 5.2, dated January 2024;
  - version 5.3, dated June 2024.

  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 v1.0.3.

Subject: Independent Auditor's Report WebTrust for CAs – S/MIME
Amstelveen, 27 March 2025

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 v1.0.3.

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.

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

Relative effectiveness of controls

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 changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period 1 January 2024 through 31 December 2024, 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 v1.0.3.

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 v1.0.3, nor the suitability of any of Logius' services for any customer's intended purpose.

Subject: Independent Auditor's Report WebTrust for CAs – S/MIME
Amstelveen, 27 March 2025

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, 27 March 2025

Original signed by

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

Subject: Independent Auditor's Report WebTrust for CAs – S/MIME
Amstelveen, 27 March 2025

Attachment A: List of CAs in scope

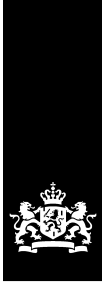
The following CAs were in scope of the WebTrust for CAs S/MIME audit:

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	54adfac79257aeca359c2e12fbe4ba5d20dc9457	3C4FB0B95AB8B30032F432B86F535FE172C185D0FD39865837CF36187FA6F428	
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:92:73:18:31:9a:ee:dd:b4:7b:1b:84:3a:2e	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2039	9bf8804e32827e7125c96ebf240e59aa447048c9	B80BF76624198A2D5D282068B49EF370AD901AB3A42897B628EFE6E6980B0A4E	
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	ff6875427dfa6fc75a93389f3544d0aa2d00b289	2E7A0A3B0C527EB20C52253C8D2278CA108136A8CA3A4EA22DA7B59BAC90650A	
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	43eb4d00d39593cea67c400d6d11be39d132aee2	D9581DBDE99B39EEFF6CE5C80DE1650DA0C1C8A109705ED286C53BC95E6655E4	
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	eeac6d40ead5046a872c557bf53f2ddaeedbace2	8222BC4FE7A3DDCA9EF0BF0D682AC888799F87822D15332A54C0BFDFC6854F7B	
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	6d1b25025de048f46e1375e257849d50f3301443	AD493D6E85EC608AB813A887BDC4D4196A0BC9B33D2565A7FA8AC430F08A99A5	
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	533cb8698896050a41739329cb22e2accd1e2160	F0305F07AB78862F2F11E4DEFE6E5EB749F8686B54613355A4845DE2052C73DE	

Subject: Independent Auditor's Report WebTrust for CAs – S/MIME
Amstelveen, 27 March 2025

Attachment B: Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Delayed S/MIME audit report for MoD PKIoverheid G3 CA	Bugzilla Ticket Link



Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius
WebTrust for CAs – S/MIME 2024

Date 14 March 2025

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 2024 through 31 December 2024

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

For the issuance of S/MIME CA services, the central infrastructure of the Dutch Government in 2024 consists of the CAs as enumerated in Attachment A. Of these CAs the Root CAs ("Staat der Nederlanden Root CA – G3", "Staat der Nederlanden - G4 Root Publ G-SMIME - 2024") and the first four listed intermediate CAs are used to issue TSP CAs which in turn can issue working S/MIME certificates. The sole exception is the "Staat der Nederlanden Autonome Apparaten CA – G3" which has only issued TSP certificates which are incapable for S/MIME. However, since the intermediate CA is unconstrained it is included in the processes and controls to which this management assertion applies. The Intermediate CAs issued in 2013 are Extant CAs per the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (SBRG) Appendix B, and as such 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 2024 to 31 December 2024, Logius has:

- disclosed its S/MIME certificate lifecycle management business practices in its Certificate Practice Statement, version 5.1 – dated October 2023, version 5.2 – dated January 2024, version 5.3 – dated June 2024

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 v1.0.3.

On behalf of

The Secretary of State of Kingdom relations and Digital development,

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	54adfac79257aeca359c2e12fbe4ba5d20dc9457	3C4FB0B95AB8B30032F432B86F535FE172C185D0FD39865837CF36187FA6F428	
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:92:73:18:31:9a:ee:dd:b4:7b:1b:84:3a:2e	RSASSA-PSS	4096 bits	sha512	23 May 2024	20 May 2039	9bf8804e32827e7125c96ebf240e59aa447048c9	B80BF76624198A2D5D282068B49EF370AD901AB3A42897B628EFE6E6980B0A4E	
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	ff6875427dfa6fc75a93389f3544d0aa2d00b289	2E7A0A3B0C527EB20C52253C8D2278CA108136A8CA3A4EA22DA7B59BAC90650A	
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	43eb4d00d39593cea67c400d6d11be39d132aee2	D9581DBDE99B39EEFF6CE5C80DE1650DA0C1C8A109705ED286C53BC95E6655E4	
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	eeac6d40ead5046a872c557bf53f2ddaeedbace2	8222BC4FE7A3DDCA9EF0BF0D682AC888799F87822D15332A54C0BFDFC6854F7B	
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	6d1b25025de048f46e1375e257849d50f3301443	AD493D6E85EC608AB813A887BDC4D4196A0BC9B33D2565A7FA8AC430F08A99A5	

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 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	F0305F07AB78862F2F11E4DEFE6E5EB749F8686B54613355A4845DE2052C73DE	

Attachment B: Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Delayed S/MIME audit report for MoD PKIoverheid G3 CA	Bugzilla Ticket Link

Page 6 of 6