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 2024

Subject: Independent Auditor's Report WebTrust for CAs Baseline Requirements

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 2023 through 31 December 2023 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 SSL certificate lifecycle management business practices in its Certification Practice Statement:
    - version 5.0, dated October 2022;
    - version 5.1, dated October 2023;

  including its commitment to provide SSL Certificates in conformity with the CA/Browser Forum Guidelines, as published on the website: https://cps.pkioverheid.nl, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities of TSPs, as 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.
- 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.

Subject: Independent Auditor Report WebTrust for CAs – SSL Baseline with Network Security
Amstelveen, 27 March 2024

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 – SSL Baseline with Network Security v2.7.

Our independence and quality control

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 and the '*Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten*' (ViO, Code of Ethics for Professional Accountants, a regulation with respect to independence) of the '*Koninklijke Nederlandse Beroepsorganisatie van Accountants*' (NBA, Royal Netherlands Institute of Chartered Accountants).

We apply the International Standard on Quality Control 1, 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 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.

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 2023 through 31 December 2023, Logius management's assertion, as referred to above, except for the effects of the matter discussed in the preceding paragraph, 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 Logius' 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 Logius' services for any customer's intended purpose.

Use of the WebTrust seal

Logius' use of the WebTrust® Principles and Criteria 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.

Subject: Independent Auditor Report WebTrust for CAs – SSL Baseline with Network Security
Amstelveen, 27 March 2024

On behalf of KPMG Advisory N.V.

Amstelveen, 27 March 2024

Digitally signed by:
Ronald Koorn
March 27 2024 3:46 PM +01:00...

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

Subject: Independent Auditor Report WebTrust for CAs – SSL Baseline with Network Security
Amstelveen, 27 March 2024

Attachment A: List of CAs in scope

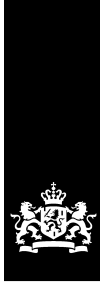
The following CAs were in scope of the WebTrust for CAs Baseline Requirements Audit:

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 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	
3	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	
4	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	
5	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	

Subject: Independent Auditor Report WebTrust for CAs – SSL Baseline with Network Security
Amstelveen, 27 March 2024

Attachment B: Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Delayed audit statements for intermediate CAs	Bugzilla Ticket Link



Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius WebTrust for CAs – SSL Baseline with Network Security 2023

Date 18 March 2024

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 2023 through 31 December 2023

LOGIUS MANAGEMENT'S ASSERTION

The Dutch Governmental Service Organisation for ICT "Logius" provides its SSL Certification Authority (CA) services known as "PKIoverheid" through the central infrastructure of the Dutch Government. For the issuance of SSL– CA services, the central infrastructure of the Dutch Government in 2023 consists of one Root CA ("Staat der Nederlanden Root CA – G3") and one intermediate CA ("Staat der Nederlanden Organisatie Services CA – G3").

The other intermediate CAs are not technically constrained but are used only for issuance of TSP CAs (issuing CAs) which in turn issue S/MIME certificates. Due to the lack of technical constraints these CAs are included in the processes and controls to which this management assertion applies.

The management of Logius has assessed its disclosures of its certificate practices and controls over its (SSL) CA services. Based on that assessment, in Logius management's opinion, in providing its SSL [and non-SSL] Certification Authority (CA) services in the Netherlands, throughout the period 1 January 2023 to 31 December 2023 for its CAs as enumerated in Attachment A, Logius has:

- disclosed its SSL certificate lifecycle management business practices in its Certificate Practice Statement (CPS, version 5.0 – dated October 2022, version 5.1 – dated October 2023) as published on the website of the Policy Authority PKIoverheid, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements, and provided such services in accordance with its disclosed practices;

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL 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 authorised individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

- 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, including the following:

CA BUSINESS PRACTICES DISCLOSURE

CA SERVICE INTEGRITY

- Key Generation Ceremony
- Certificate Content And Profile
- Certificate Request Requirements
- Verification Practices
- Certificate Revocation And Status Checking
- Employee And Third Parties
- Data Records
- Audit

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 CAs Baseline Requirements 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 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	
3	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	
4	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	

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
5	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	

Attachment B: Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Delayed audit statements for intermediate CAs	Bugzilla Ticket Link