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

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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certificate Practice Statement:
  - version 5.0, dated October 2022;
  - version 5.1, dated October 2023;

  as published on the website: https://cps.pkioverheid.nl/.
- 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 – June 2021.

Logius makes use of external registration authorities ("TSPs" in PKIoverheid) 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 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, 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, 27 March 2024

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, 27 March 2024

Digitally signed by:
Ronald Koorn
March 27 2024 3:47 PM +01:00...

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

Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 27 March 2024

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	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	
6	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	
7	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	

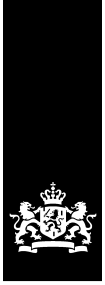
Subject: Independent Auditor's Report WebTrust for CAs
Amstelveen, 27 March 2024

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
8	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	257906c6a631fddf9e71a0fe4b31371710ee46bc	BF45E3CE00CF22B8FC505BCA3875C6C85BC4FF5F2D9B439180829963307D8DC9	
9	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	6d1b25025de048f46e1375e257849d50f3301443	F0305F07AB78862F2F11E4DEFE6E5EB749F8686B54613355A4845DE2052C73DE	

Subject: Independent Auditor's Report WebTrust for CAs
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 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 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 (CPS, version 5.0 – dated October 2022, version 5.1 – dated October 2023), 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 life cycle 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 2023 to 31 December 2023 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 Certification Practice Statement, as published on the website of the Policy Authority PKIoverheid and provided such services in accordance with its disclosed practices;
- Maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their life cycles;

  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - 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 & 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 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 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	
6	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	

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint	Other information
7	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	
8	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	257906c6a631fddf9e71a0fe4b31371710ee46bc	BF45E3CE00CF22B8FC505BCA3875C6C85BC4FF5F2D9B439180829963307D8DC9	
9	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	6d1b25025de048f46e1375e257849d50f3301443	F0305F07AB78862F2F11E4DEFE6E5EB749F8686B54613355A4845DE2052C73DE	

Attachment B: Publicly disclosed incidents

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

Page 7 of 7