KPMG

KPMG Advisory N.V.
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

Independent Auditor's Report

Amstelveen, 2 February 2018

To the Management of Logius

We have examined the assertion by the management of Logius, regarding the disclosure of its key and certificate life cycle management business practices and the effectiveness of its controls over key and SSL certificate integrity, the authenticity of subscriber information, logical and physical access to CA systems and data, the continuity of key and certificate life cycle management operations, and development, maintenance and operation of systems integrity, based on the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security – Version 2.2, during the period from 1 January 2017 through 31 December 2017, for the following CA's (referred to collectively as the Central Infrastructure of the Dutch Government PKI "PKIoverheid"):

Certificate Authority	SHA2-fingerprint
Root Certification Authority – G2 ("Staat der Nederlanden Root CA – G2")	66:8C:83:94:7D:A6:3B:72:4B:EC:E1:74:3C:31:A0:E6:AE:D0:DB:8E:C5:B3:1B:E3:77:BB:78:4F:91:B6:71:6F
Subordinate Domain-CA for Organisations – G2 ("Staat der Nederlanden Organisatie CA – G2")	85:A8:F5:86:6D:D7:8D:F1:73:B0:66:73:17:C5:9B:2D:62:42:DE:59:EB:01:BB:2F:2E:8B:9D:B7:14:B4:CA:27
Root Certification Authority – G3 ("Staat der Nederlanden Root CA – G3")	3C:4F:B0:B9:5A:B8:B3:00:32:F4:32:B8:6F:53:5F:E1:72:C1:85:D0:FD:39:86:58:37:CF:36:18:7F:A6:F4:28
Subordinate Domain-CA for Organisations-Services – G3 ("Staat der Nederlanden Organisatie Services CA – G3")	D9:58:1D:BD:E9:9B:39:EE:FF:6C:E5:C8:0D:E1:65:0D:A0:C1:C8:A1:09:70:5E:D2:86:C5:3B:C9:5E:66:55:E4

The management of Logius is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included:

- Obtaining an understanding of CA's key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity;
- Selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management business practices;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

Through the Central Infrastructure of the Dutch Government PKI "PKIoverheid", Logius provides certificates to subordinate Certification Services Providers (CSPs) in order to become part of the Dutch Government PKI "PKIoverheid". The relative effectiveness and significance of specific controls at the Central Infrastructure of the Dutch Government PKI "PKIoverheid" 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 subordinate Certification Service Providers operating within the Dutch Government PKI and their individual subscriber and relying party locations. During our examination, we have performed no procedures to evaluate the effectiveness of controls at these locations.

Because of the nature and inherent limitations of controls, Logius' ability to meet the afore-mentioned criteria may be affected. 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.

As stated by Logius in the Management Assertion, the Root Certification Authority – G2 ("Staat der Nederlanden Root CA - G2") and the Subordinate Domain-CA for Organisations – G2 ("Staat der Nederlanden Organisatie CA - G2") do not provide revocation information via an Online Certificate Status Protocol (OCSP) service (the recently established G3 Root CA and Subordinate Domain-CA provide OCSP services).

Subject: Independent Auditor Report
Amstelveen, 2 February 2018

In our opinion, for the period 1 January 2017 through 31 December 2017, Logius management's assertion, as set forth above, except for the effects of the matter discussed in the preceding paragraph, is fairly stated and in all material respects has:

- Disclosed its Certificate practices and procedures in its Certification Practice Statement, version 4.0, dated October 2016, including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines and
- Maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security – Version 2.2.

The WebTrust seal of assurance for Certification Authorities on the Logius' website 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.

This report does not include any representation as to the quality of the certification services of Logius beyond those covered by the WebTrust® for Certification Authorities – Baseline Requirements, nor the suitability of any services of Logius for any customer's intended purpose.

On behalf of KPMG Advisory N.V.

Original signed by

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

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius 2017

Date 1 February 2018

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 2017 through 31 December 2017

1 February 2018

The Dutch Governmental Shared Service Organisation for ICT “Logius” provides its SSL Certification Authority (CA) services through the central infrastructure of the Dutch Government. For the issuance of SSL – CA services, the central infrastructure of the Dutch Government consists:

- Root Certification Authority - G2 (“Staat der Nederlanden Root CA – G2”)
  - Subordinate Domain-CA for Organisations - G2 (“Staat der Nederlanden Organisatie CA – G2”);

- Root Certification Authority – G3 (“Staat der Nederlanden Root CA – G3”)
  - Subordinate Domain-CA for Organisations-Services – G3 (“Staat der Nederlanden Organisatie Services CA – G3”);

The management of Logius has assessed the disclosure of its certificate practices and its controls over its SSL CA services. Based on that assessment, in Management’s opinion, in providing its SSL CA services in the Netherlands, during the period from 1 January 2017 through 31 December 2017, Logius has:

- Disclosed its Certificate practices and procedures in its Certification Practice Statement, version 4.0, dated October 2016, including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines and

- Maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security – Version 2.2, including the following:

- **CA BUSINESS PRACTICES DISCLOSURE**

- **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

- **CA ENVIRONMENTAL SECURITY**

Within the G2 hierarchy, Logius does not operate an OCSP responder to serve status information on the subordinate CAs. The rationale for this decision is that the inception of this environment predates the effective date of the Baseline Requirements by four years. Logius has incorporated OCSP functionality in the G3 CA, which is the successor of the G2 Root. In both environments status information is made available by means of Certificate Revocation Lists.

For approval:

Original signed by

ir. Y.L. van der Brugge-Wolring
General Director Logius