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, that in providing its Certification Authority (CA) services in the Netherlands during the period from 1 January 2017 through 31 December 2017, Logius has:

— Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement, version 4.0, dated October 2016, 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 CSP'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, version 2.0 – March 2011 for the following CAs (referred to collectively as the Central Infrastructure of the Dutch Government PKI "PKIoverheid"):

Subject: Independent Auditor Report
Amstelveen, 2 February 2018

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 Government-Citizen – G2 (“Staat der Nederlanden Burger CA – G2”)	2F:2F:0C:84:4F:B3:36:A9:42:1A:B6:FA:36:DC:DA:C3:BB:84:E0:38:4C:FF:5D:AD:51:11:3C:8C:A4:24:E6:A4
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
Subordinate Domain-CA for Autonomous Devices – G2 (“Staat der Nederlanden Autonome Apparaten CA – G2”)	1B:17:10:02:64:24:7D:70:90:03:61:16:23:8C:93:F4:58:53:ED:E5:AE:A6:F9:F1:A4:52:4F:69:78:DD:89:54
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 Government-Citizen – G3 (“Staat der Nederlanden Burger CA – G3”)	2E:7A:0A:3B:0C:52:7E:B2:0C:52:25:3C:8D:22:78:CA:10:81:36:A8:CA:3A:4E:A2:2D:A7:B5:9B:AC:90:65:0A
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
Subordinate Domain-CA for Organisations-Persons – G3 (“Staat der Nederlanden Organisatie Persoon CA – G3”)	82:22:BC:4F:E7:A3:DD:CA:9E:F0:BF:0D:68:2A:C8:88:79:9F:87:82:2D:15:33:2A:54:C0:BF:DF:C6:85:4F:7B
Subordinate Domain-CA for Autonomous Devices – G3 (“Staat der Nederlanden Autonome Apparaten CA – G3”)	AD:49:3D:6E:85:EC:60:8A:B8:13:A8:87:BD:C4:D4:19:6A:0B:C9:B3:3D:25:65:A7:FA:8A:C4:30:F0:8A:99:A5

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:

Subject: Independent Auditor Report
Amstelveen, 2 February 2018

— Obtaining an understanding of the CA key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance and operation of CA-systems;

— Selectively testing transactions executed in accordance with disclosed key and 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.

In our opinion, for the period 1 January 2017 through 31 December 2017, Logius management's assertion, as set forth above, is fairly stated, in all material respects, based on the WebTrust® Principles and Criteria for Certification Authorities, version 2.0 – March 2011.

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.

Subject: Independent Auditor Report
Amstelveen, 2 February 2018

This report does not include any representation as to the services of Logius beyond those covered by the WebTrust® Principles and Criteria for Certification Authorities, 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 the following Certification Authority (CA) services through the central infrastructure of the Dutch Government:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate suspension
- Certificate status information processing (using an online repository)

The central infrastructure of the Dutch Government consists of the following entities:

- Root Certification Authority (“Staat der Nederlanden Root CA”)
  - Subordinate Domain-CA for Government-Citizen (“Staat der Nederlanden Burger CA”);
  - Subordinate Domain-CA for Government and Businesses (“Staat der Nederlanden Overheid CA”).
- Root Certification Authority – G2 (“Staat der Nederlanden Root CA – G2”)
  - Subordinate Domain-CA for Government-Citizen – G2 (“Staat der Nederlanden Burger CA - G2”);
  - Subordinate Domain-CA for Organisations - G2 (“Staat der Nederlanden Organisatie CA - G2”);
  - Subordinate Domain-CA for Autonomous Devices - G2 (“Staat der Nederlanden Autonome Apparaten CA – G2”).
- Root Certification Authority – G3 (“Staat der Nederlanden Root CA – G3”)
  - Subordinate Domain-CA for Government-Citizen – G3 (“Staat der Nederlanden Burger CA – G3”);
  - Subordinate Domain-CA for Organisations-Services – G3 (“Staat der Nederlanden Organisatie Services CA – G3”);
  - Subordinate Domain-CA for Organisations-Persons – G3 (“Staat der Nederlanden Organisatie Persoon CA – G3”);
  - Subordinate Domain-CA for Autonomous Devices – G3 (“Staat der Nederlanden Autonome Apparaten CA – G3”).

Logius provides certificates to Certification Services Providers (CSPs) in order to become part of the Dutch Government PKI "PKIoverheid". The practices outlining the processes related to accession, supervision and control are described in the PKIoverheid Certification Practice Statement (CPS, version 4.0, dated October 2016), 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 provide only reasonable assurance with respect to CA operations of Logius. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of Logius has assessed the controls over the CA operations of PKIoverheid. Based on that assessment, in Management's opinion, in providing CA services in the Netherlands, during the period from 1 January 2017 through 31 December 2017, 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 CSP'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, version 2.0 – March 2011 including the following:

CA BUSINESS PRACTICES DISCLOSURE

- Certification Practice Statement (CPS)
- Certificate Policy (if applicable)

CA BUSINESS PRACTICES MANAGEMENT

- Certificate Policy Management (if applicable)
- Certification Practice Statement Management
- CP and CPS Consistency (if applicable)

CA ENVIRONMENTAL CONTROLS

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA KEY LIFE CYCLE 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 Life Cycle Management
- CA Key Escrow (if applicable)

SUBSCRIBER KEY LIFE CYCLE MANAGEMENT CONTROLS

- CA-Provided Subscriber Key Generation Services (if supported)
- CA-Provided Subscriber Key Storage and Recovery Services (if supported)
- Integrated Circuit Card (ICC) Life Cycle Management (if supported)
- Requirements for Subscriber Key Management

CERTIFICATE LIFE CYCLE MANAGEMENT CONTROLS

- Subscriber Registration
- Certificate Renewal (if supported)
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension (if supported)
- Certificate Validation

SUBORDINATE CA CERTIFICATE LIFE CYCLE MANAGEMENT CONTROLS

- Subordinate CA Certificate Life Cycle Management

For approval:

Original signed by

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