Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius 2014

Date 3 March 2015

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 2014 through 31 December 2014

3 March 2015

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 3.8, dated 1 July 2014), 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 maintainning 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 2014 through 31 December 2014, 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:

Drs. S.B. Luitjens
Directeu

KPMG IT Auditors
P.O. Box 43004
3540 AA Utrecht
The Netherlands

Rijnzathe 14
3454 PV De Meern
The Netherlands
Telephone +31 (0)30 658 2150
Fax +31 (0)30 658 2199

Independent Auditor's Report

Utrecht, 3 March 2015

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 2014 through 31 December 2014, Logius has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement, version 3.8, dated 1 July 2014, 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"):

- 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").

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 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 2014 through 31 December 2014, 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.

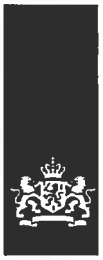
This report does not include any representation as to the services of Logius beyond those covered by the WebTrust® Principles and Criteria for Certification Authorities, nor the suitability of any services of Logius for any customer's intended purpose.

On behalf of KPMG Advisory N.V.

Utrecht, 3 March 2015

drs. ing. R.F. Koorn RE CISA

Partner



Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius 2014

Date 3 March 2015

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 2014 through 31 December 2014

3 March 2015

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 2014 through 31 December 2014, Logius has:

- Disclosed its Certificate practices and procedures in its Certification Practice Statement, version 3.8, dated 1 July 2014, 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, version 1.1 – January 2013, 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

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:

Drs. S.B. Luitjens
Director

KPMG IT Auditors
P.O. Box 43004
3540 AA Utrecht
The Netherlands

Rijnzathe 14
3454 PV De Meern
The Netherlands
Telephone +31 (0)30 658 2150
Fax +31 (0)30 658 2199

Independent Auditor's Report

Utrecht, 3 March 2015

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, version 1.1 – January 2013, during the period from 1 January 2014 through 31 December 2014, for the following CA's (referred to collectively as the Central Infrastructure of the Dutch Government PKI "PKIoverheid"):

- 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 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) .

In our opinion, for the period 1 January 2014 through 31 December 2014, 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 3.8, dated 1 July 2014, 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, versie 1.1.

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.

Utrecht, 3 March 2015

drs. ing. R.F. Koorn RE CISA

Partner

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius EV 2014

Date 3 March 2015

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Extended Validation Certification Authority Operations during the period from 1 January 2014 through 31 December 2014

3 March 2015

The Dutch Governmental Shared Service Organisation for ICT "Logius" (Logius), provides Extended Validation Certification Authority (EV-CA) services through its "Staat der Nederlanden EV CA", consisting of a root Certification Authority and one subordinate CA.

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 Extended Validation Certification Practice Statement (CPS, version 1.3, dated 1 July 2014), as is published on the website of the Policy Authority PKIoverheid.

The management of Logius is responsible for the Extended Validation Certification Authority of the Dutch Government PKI and responsible for establishing and maintaining effective controls over its EV-CA operations, including:

- CA Business Practices Disclosure in its Certificate Practice Statement, as published on the website of Logius.
- Service integrity, including key and certificate life cycle management controls.

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 the EV-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 EV-CA operations of PKIoverheid. Based on that assessment, in Management's opinion, in providing EV-CA services in the Netherlands, during the period from 1 January 2014 through 31 December 2014, Logius has:

- Disclosed its EV Certificate life cycle management practices and procedures, including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with its disclosed practices, and
- Maintained effective controls to provide reasonable assurance that:
  - EV Subscriber information was properly collected, authenticated and verified, and
  - The integrity of keys and EV certificates it manages is established and protected throughout their life cycles,

based on the WebTrust® Principles and Criteria for Certification Authorities - Extended Validation SSL, version 1.4.5 – April 2014 including the following:

- **CA BUSINESS PRACTICES DISCLOSURE**

- **SERVICE INTEGRITY**
  - EV Certificate Content and Profile
  - EV Certificate Request Requirements
  - Information Verification Requirements
  - Certificate Status Checking and Revocation
  - Employee and Third Party Issues
  - Data and Record Issues

For approval:

Drs. S.B. Luitjens
Director

KPMG IT Auditors
P.O. Box 43004
3540 AA Utrecht
The Netherlands

Rijnzathe 14
3454 PV De Meern
The Netherlands
Telephone +31 (0)30 658 2150
Fax +31 (0)30 658 2199

Independent Auditor's Report

Utrecht, 3 March 2015

To the Management of Logius:

We have examined the assertion by the management of Logius, that in providing its Extended Validation Certification Authority (EV-CA) services in the Netherlands during the period from 1 January 2014 through 31 December 2014, Logius has:

- Disclosed its EV Certificate life cycle management practices and procedures, including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
  - EV Subscriber information was properly collected, authenticated (for the registration activities performed by Logius) and verified; and
  - The integrity of keys and EV certificates it manages is established and protected throughout their life cycles;

in accordance with the WebTrust® Principles and Criteria for Certification Authorities - Extended Validation SSL, version 1.4.5 for the following CAs (referred to collectively as the Central Infrastructure of the Dutch Government PKI "PKIoverheid"):

- Root Certificate Authority ("Staat der Nederlanden EV Root CA")
  - Subordinate CA ("Staat der Nederlanden EV Intermediair CA")

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 International Assurance Engagement Standards and, accordingly, included:

- Obtaining an understanding of CA's key and EV certificate life cycle management business practices and its controls over key and EV 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 EV 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 aforementioned 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 2014 through 31 December 2014, 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 - Extended Validation SSL, version 1.4.5.

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.

The WebTrust for EV 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 Logius' services beyond those covered by the WebTrust® Principles and Criteria for Certification Authorities - Extended Validation Audit Criteria, nor the suitability of any services for any customer's intended purpose.

On behalf of KPMG Advisory N.V.

Utrecht, 3 maart 2015

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