KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountant's Report

To the Management of Symantec Corporation:

We have examined the assertions by the management of Symantec Corporation ("Symantec") and Verisign, Inc. ("Verisign"), an independent service organization that provides data center hosting services to Symantec, for its Symantec Non-Federal Shared Service Provider CA services at Mountain View, California and New Castle, Delaware regarding the disclosure of its business, key life cycle management, certificate life cycle management, and CA environmental control practices, the provision of services in accordance with its Certification Practice Statement, and the effectiveness of 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 CA systems integrity throughout the period from December 1, 2014 to November 30, 2015 for Symantec's VeriSign Class 3 SSP Intermediate CA - G2, Symantec Class 1 SSP CA - G2, Symantec Class 2 SSP CA - G2, Symantec Class 3 SSP Intermediate CA - G3, and the Symantec Non-Federal SSP – customer specific CAs (collectively referred to as the "Non-Federal SSP CAs").

The management of Symantec and Verisign are responsible for their respective assertions. Our responsibility is to express an opinion, based on our examination.

Symantec makes use of external registration authorities for specific subscriber registration activities for the Non-Federal SSP – customer specific CAs as disclosed in its Non-Federal SSP CPS on Symantec's website. Our examination did not extend to the controls of external registration authorities.

Our examination, which commenced on October 16, 2015 and ended on May 13, 2016, was conducted in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of Symantec's 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 our examination provides a reasonable basis for our opinion. The relative effectiveness and significance of specific controls at Symantec and Verisign 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.

Because of the nature and inherent limitations of controls, Symantec and Verisign's 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.

We noted the following issue that resulted in a modification of our opinion:

Principle 3, criterion 3.10 requires that the CA maintains controls to provide reasonable assurance that:

- significant CA environmental, key management, and certificate management events are accurately logged;
- the confidentiality and integrity of current and archived audit logs are maintained;
- audit logs are completely and confidentially archived in accordance with disclosed business practices; and
- audit logs are reviewed periodically by authorized personnel.

During our examination, we noted that visitor entry and exit logs for a Symantec CA facility were not archived for a minimum of 10 years and 6 months, as specified in Symantec's Non-Federal SSP CPS. As a result, we noted that Symantec had not maintained effective controls to meet Principle 3, Criterion 3.10 with respect to the retention of CA facility entry and exit logs.

In our opinion, except for the matters described in the preceding paragraphs, in providing its Symantec Non-Federal SSP CA services at Mountain View, California and New Castle, Delaware, USA, during the period December 1, 2014 to November 30, 2015 -

- Symantec disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013 ("Non-Federal SSP CPS"), for the Symantec Non-Federal SSP CAs (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9) on Symantec's website
- Symantec provided its CA services in accordance with its disclosed practices, including:
  - Non-Federal SSP CPS (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- Symantec 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 performed by Symantec); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- Symantec and Verisign[1] 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 v2.0.

This report does not include any representation as to the quality of Symantec's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of Symantec's services for any customer's intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, CA
May 13, 2016

[1] Limited to only physical access to CA systems and data hosted within the VeriSign data center in New Castle, Delaware

Assertion by Management as to
Its Disclosure of its Business Practices and its Controls
Over its Certification Authority Operations
During the period from December 1, 2014 through November 30, 2015

May 13, 2016

Symantec Corporation ("Symantec") provides the following certification services through Symantec's VeriSign Class 3 SSP Intermediate CA – G2, Symantec Class 1 SSP CA – G2, Symantec Class 2 SSP CA – G2, Symantec Class 3 SSP Intermediate CA – G3, and the Symantec Non-Federal SSP – customer specific CAs (collectively referred to as the "Non-Federal SSP CAs"):

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

Management of Symantec is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013 ("Non-Federal SSP CPS"), on Symantec's website, 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.

Controls have inherent limitations, 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 Symantec's Non-Federal SSP CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its Non-Federal SSP CA operations. Based on that assessment, in Management's opinion, in providing its Non-Federal SSP CA services at Mountain View, California, USA and New Castle, Delaware, USA, during the period from December 1, 2014 through November 30, 2015 –

- Symantec disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013 ("Non-Federal SSP CPS"), for the Symantec Non-Federal SSP CAs (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9) on Symantec's website
- Symantec provided its CA services in accordance with its disclosed practices including:
  - Non-Federal SSP CPS (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- Symantec maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - the Subscriber information was properly authenticated (for the registration activities performed by Symantec); and

  - subordinate CA certificate requests were accurate, authenticated, and approved
- Symantec maintained effective controls to provide reasonable assurance that
  - 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 v2.0, including the following:

CA Business Practices Disclosure
- Certification Practice Statement

CA Business Practices Management
- Certification Practice Statement Management

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

Subscriber Key Life Cycle Management Controls
- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls
- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls
- Subordinate CA Certificate Life Cycle Management

except for the effects of the matter noted below:

Principle 3, Criterion 3.10 Audit Logging of WebTrust for CAs requires that the CA maintains controls to provide reasonable assurance that:

- significant CA environmental, key management, and certificate management events are accurately and appropriately logged;
- the confidentiality and integrity of current and archived audit logs are maintained;
- audit logs are completely and confidentially archived in accordance with disclosed business practices; and
- audit logs are reviewed periodically by authorized personnel.

Visitor entry and exit logs for a Symantec CA facility were not archived for a minimum of 10 years and 6 months, as specified in Symantec's Non-Federal SSP CPS, to meet Principle 3, Criterion 3.10.

Access log retention requirements for Symantec CA facilities exceed Symantec Corporate Security requirements. Due to recent personnel changes within the Corporate team that manages data retention across the company, CA facility log retention periods were reduced to match Corporate security log retention requirements. Upon identification and communication of the issue, the retention periods of physical access logs have since been updated to comply with the respective requirements for CA facilities. In addition, safeguards will be put in place to require supplemental approval and periodic monitoring of data retention requirements moving forward.

Symantec Corporation

Nicolas Popp
Vice President, User Authentication

Assertion by Management of Verisign, Inc.
Regarding its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
During the Period December 1, 2014 through November 30, 2015

May 13, 2016

Verisign, Inc. an independent service organization (sub-service provider), provides data center hosting services to Symantec Corporation ("Symantec") for Symantec Certification Authorities (CAs) hosted in New Castle, Delaware.

Management of Verisign is responsible for establishing and maintaining effective controls over its data center hosting services for Symantec CAs hosted in New Castle, Delaware including CA environmental controls (limited to physical and environmental security). These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal control can provide only reasonable assurance with respect to Verisign's data center hosting services for Symantec CAs hosted in New Castle, Delaware. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its data center hosting services for Symantec CA operations. Based on that assessment, to the best of our knowledge and belief, we confirm that in providing its data center hosting services in New Castle, Delaware during the period December 1, 2014 through November 30, 2015, Verisign has

- Maintained effective controls to provide reasonable assurance that
  - Physical access to Symantec CA systems and data was restricted to authorized individuals

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0 including the following:

CA Environmental Controls

- Physical and Environmental Security

Verisign, Inc.

Joseph David Pool
Senior Vice President of Architecture & Tech Services