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 Certification Authority (CA) operations at Mountain View, California, USA and New Castle, Delaware, regarding the disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, the consistency of its Certification Practice Statement with its Certificate Policy, the provision of services in accordance with its Certificate Policy and 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 the Symantec owned Root Certification Authority – Class 3 Public Primary Certification Authority.

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

We conducted our examination 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 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 issues that resulted in a modification of our opinion:

Impacted WebTrust for CAs Criteria		Issues Noted
2.2	The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.	During our examination, we noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the STN CPS. This caused WebTrust for CAs Criterion 2.2 to not be met.
3.10	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 physical access entry and exit logs for a CA facility were not archived for 7 years as specified in the STN CPS. This caused WebTrust for CAs Criterion 3.10 to not be met 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 CA services for the Class 3 Public Primary Certification Authority in Mountain View, California, USA and New Castle, Delaware, USA during the period to December 1, 2014 to November 30, 2015,

- Symantec disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Symantec Trust Network Certificate Policy, Version 2.8.17, dated November 30, 2015 ("STN CP") and Symantec Trust Network Certification Practice Statement, Version 3.8.21, dated November 25, 2015 ("STN CPS") on Symantec's website
- Symantec maintained effective controls to provide reasonable assurance that:
  - Symantec's Certification Practice Statement is consistent with its Certificate Policy
  - Symantec provides its services in accordance with Symantec's Certification Practice Statement and its Certificate Policy
- Symantec maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles 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, California
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 its Symantec owned Root Certification Authority – Class 3 Public Primary Certification Authority:

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

Management of Symantec is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure in its STN CPS on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, and certificate lifecycle management 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 the Symantec and Verisign CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed its controls over its Symantec CA operations. Based on that assessment, in Symantec management's opinion, in providing its Symantec CA services for the Class 3 Public Primary Certification Authority at Mountain View, California, USA and New Castle, Delaware, USA, during the period December 1, 2014 through November 30, 2015 -

- Symantec disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Symantec Trust Network Certificate Policy, Version 2.8.17, dated November 30, 2015 ("STN CP") and Symantec Trust Network Certification Practice Statement, Version 3.8.21, dated November 25, 2015 ("STN CPS") on Symantec's website
- Symantec maintained effective controls to provide reasonable assurance that:
  - Symantec's Certification Practice Statement was consistent with its Certificate Policy
  - Symantec provided its services in accordance with its Certificate Policy and Certification Practice Statement
- 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 and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- Symantec and Verisign 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, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice 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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

except for the effects of the matters noted below:

Impacted WebTrust for CAs Criteria		Issues Noted
2.2	The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.	It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the STN CPS. HR has performed a validation of personnel requiring Trusted Status is in the process of completing reinvestigations on all required individuals. Management has also reiterated internal procedures to ensure that all reinvestigations are consistently performed.
3.10	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.	It was noted that physical access entry and exit logs for a CA facility were not archived for a minimum of 7 years, as specified in the 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 without approval from the Symantec Website Security business unit. 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, policy updates have been put in place to require supplemental approval and periodic monitoring of data retention requirements moving forward.

Symantec Corporation

Roxane Divol
Senior Vice President of Trust Services