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"), 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® for Certification Authorities – SSL Baseline with Network Security Requirements Audit Criteria v2.0, during the period December 1, 2014 through November 30, 2015, for the STN and Thawte SSL CAs listed in Appendix A.

The management of Symantec and Verisign are responsible for their respective assertions. Our responsibility is to express an opinion on management assertions 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 Symantec's key and SSL certificate life cycle management business practices and its controls over
  - The key and SSL certificate integrity;
  - The continuity of key and certificate life cycle management operations;
  - 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.

The relative effectiveness and significance of specific controls at Symantec 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, the ability of Symantec and VeriSign 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
1	Principle 2, Criterion 2.2 requires that the CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following: • As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA shall notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. • Also as of the Effective Date, the CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a SubjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name. (See SSL Baseline Requirements Section 9.2.6)	During the examination period, limited instances were identified where SSL certificates were issued with an Expiry Date later than November 1, 2015 and with a SubjectAlternativeName extension or Subject commonName field containing an Internal Server Name. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 2, Criterion 2.2 to not be met.
2	Principle 2, Criterion 4.1 requires that the CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate.	During our examination, we noted that STN and Thawte Issuing SSL CAs were used to issue certificates for Symantec internal testing purposes for registered domains that Symantec did not own. As required by the CPS, Symantec did not obtain the required authorization from the respective registered domain owners prior to certificate issuance. Furthermore, certificates were also issued for internal testing purposes to unregistered domains. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 2, Criteria 4.1 to not be met.

Impacted WebTrust for CAs Criteria		Issues Noted
3	Principle 2, Criterion 7.2 requires that the CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	During our examination, we noted that physical access entry and exit logs for a CA facility were not archived for 7 years as required by Criterion 7.2, the STN CPS, and the Thawte CPS. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 2, Criterion 7.2 to not be met with respect to the retention of CA facility entry and exit logs.
4	Principle 3, Criterion 8 requires that the CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals. Such controls must include, but are not limited to: • network security and firewall management, including port restrictions and IP address filtering and • logical access controls, activity logging (WTCA 2.0 Section 3.10), and inactivity time-outs to provide individual accountability.	During our examination, we noted that access to the CA applications to issue production certificates was not restricted to authorized members of the Certificate Authentication Services team and also included other Symantec employees for testing purposes. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 3, Criterion 8 to not be met with respect to CA applications.

Impacted WebTrust for CAs Criteria		Issues Noted
5	Principle 4, Criterion 3 requires that the CA maintains controls to provide reasonable assurance that: • Certificate Systems under the control of CA capable of monitoring and logging system activity and are configured to continuously monitor and log system activity; • Automated mechanisms under the control of CA are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events; • Trusted Role personnel follows up on alerts of possible Critical Security Events; • A human review of application and system logs is performed at least every 30 days and includes: o Validating the integrity of logging processes o Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly; and • Maintain, archive, and retain logs in accordance with disclosed business practices.	Although logging was in place for selected in-scope systems, a process for periodically validating the integrity and effectiveness of the process, whereby a human review of application and system logs is performed at least every 30 days in accordance with CA Browser Forum Network Security requirements, was not in place during the examination period. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 4, Criteria 3 to not be met during the examination period.

In our opinion, except for the effects of the matter(s) discussed in the preceding paragraphs, in providing its Symantec SSL Certification Authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Cape Town, South Africa; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, during the period December 1, 2014 through November 30, 2015,

- Symantec disclosed its Certificate practices and procedures in its:
  - Symantec Trust Network Certification Practice Statement, Version 3.8.21, dated November 25, 2015 ("STN CPS") and Symantec Certificate Policy, Version 2.8.17, dated November 30, 2015 ("STN CP") on the Symantec website
  - Thawte Certification Practice Statement ("CPS"), Version 3.7.14, dated September 24, 2015 ("Thawte CPS") on Symantec's Thawte website

  including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements and provided such services in accordance with its disclosed practices
- Symantec and Verisign[1] maintained effective controls to provide reasonable assurance that:
  - SSL subscriber information was properly collected, authenticated (for the registration activities performed by Symantec) and verified;

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

- the integrity of keys and SSL 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 with Network Security v2.0, for the STN and Thawte SSL CAs.

This report does not include any representation as to the quality of Symantec's certification services beyond those covered by the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Audit Criteria, v2.0, nor the suitability of any of Symantec's services for any customers intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, California
May 13, 2016

APPENDIX A – STN and Thawte SSL CAs

Symantec Root CAs:

- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Authorized Code Signing Root CA for Microsoft
- VeriSign Universal Root Certification Authority
- Symantec Class 1 Public Primary Certification Authority - G4
- Symantec Class 2 Public Primary Certification Authority - G4
- Symantec Class 3 Public Primary Certification Authority - G4
- Symantec Class 1 Public Primary Certification Authority - G6
- Symantec Class 2 Public Primary Certification Authority - G6
- Symantec Class 3 Public Primary Certification Authority - G6
- Symantec Class 1 Public Primary Certification Authority - G7
- Symantec Class 2 Public Primary Certification Authority - G7
- Symantec Class 3 Public Primary Certification Authority - G7

Thawte Root CAs:

- thawte Primary Root CA
- thawte Primary Root CA - G2
- thawte Primary Root CA - G3
- thawte Primary Root CA - G4

Symantec SSL Issuing CAs:

- VeriSign Class 3 International Server CA - G3
- VeriSign Class 3 Secure Server CA – G3
- VeriSign Class 3 Secure Server CA - T1
- VeriSign Class 3 International Server CA - T1
- Symantec Class 3 Secure Server CA - G4
- Symantec Class 3 DSA SSL CA
- Symantec Class 3 ECC 256 bit SSL CA
- Symantec Class 3 Secure Server SHA256 SSL CA
- Symantec Class 3 ECC 256 bit SSL CA - G2
- VeriSign Class 3 Extended Validation SSL CA
- VeriSign Class 3 Extended Validation SSL SGC CA
- VeriSign Class 3 Extended Validation CA - T1
- VeriSign Class 3 Extended Validation SGC CA - T1
- Symantec Class 3 DSA EV SSL CA
- Symantec Class 3 ECC 256 bit Extended Validation CA
- Symantec Class 3 EV SSL CA - G2
- Symantec Class 3 EV SSL CA - G3
- Symantec Class 3 EV SSL SGC CA - G2
- Symantec Class 3 Extended Validation SHA256 SSL CA
- Symantec Class 3 ECC 256 bit EV CA - G2

Thawte SSL Issuing CAs:

- Thawte SSL CA
- Thawte DV SSL CA
- Thawte SGC CA - G2
- thawte SSL CA - G2
- Thawte DSA CA
- Thawte SHA256 SSL CA
- thawte DV SSL SHA256 CA
- thawte DV SSL CA - G2
- Thawte Extended Validation SSL CA
- thawte EV SSL CA - G2
- thawte EV SSL CA - G3
- Thawte Extended Validation SHA256 SSL CA

Assertion of 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, Inc. ("Symantec") provides its Symantec SSL certification authority (CA) services through the STN and Thawte SSL CAs listed in **Appendix A**.

The management of Symantec has assessed the disclosure of its certificate practices and its controls over its STN and Thawte SSL CAs services. Based on that assessment, in Symantec Management's opinion, in providing its STN and Thawte SSL CAs services at Mountain View, California, USA; New Castle, Delaware, USA; Cape Town, South Africa; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, during the period from December 1, 2014 through November 30, 2015:

- Symantec disclosed its Certificate practices and procedures in its:
  - Symantec Trust Network Certification Practice Statement, Version 3.8.21, dated November 25, 2015 ("STN CPS") and Symantec Certificate Policy, Version 2.8.17, dated November 30, 2015 ("STN CP") on the Symantec website
  - Thawte Certification Practice Statement ("CPS"), Version 3.7.14, dated September 24, 2015 ("Thawte CPS") on Symantec's Thawte website

  including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements and provided such services in accordance with its disclosed practices
- Symantec maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by Symantec) 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 with Network Security v2.0 except for the effects of the matters noted below:

Impacted WebTrust for CAs Criteria		Issues Noted
1	Principle 2, Criterion 2.2 requires that the CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following: • As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA shall notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. • Also as of the Effective Date, the CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a SubjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name. (See SSL Baseline Requirements Section 9.2.6)	It was noted that during the examination period, limited instances were identified where SSL certificates were issued with an Expiry Date later than November 1, 2015 and with a SubjectAlternativeName extension or Subject commonName field containing an Internal Server Name. The noted certificates have since expired or have been revoked. We have also implemented additional pre-issuance compliance checks.

Impacted WebTrust for CAs Criteria		Issues Noted
2	Principle 2, Criterion 4.1 requires that the CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate.	It was noted that STN Issuing SSL CAs were used to issue certificates for Symantec internal testing purposes for registered domains that Symantec did not own. As required by the CPS, Symantec did not obtain the required authorization from the respective registered domain owners prior to certificate issuance. Furthermore, certificates were also issued for testing to unregistered domains. As we disclosed in our published incident reports, Symantec has since completed a thorough investigation of its test certificates. Symantec's investigation uncovered no evidence of malicious intent, nor inappropriate use of these certificates to anyone. Each of these test certificates was issued solely for internal Symantec testing purposes that have since been revoked or have expired. Symantec has contacted the relevant domain owners and provided relevant information to the browser community to enable the browsers to evaluate the appropriateness of blacklisting these test certificates where they deemed appropriate. We have also disabled access to technical features that enabled mis-issuance of test certificates; we updated our policies, internal procedures and trainings to clarify the April 2014 change in the Baseline Requirements that removed authorization to issue certificates to unregistered domains; we updated our internal policies, procedures and trainings to strongly reinforce that test certificates must follow the same authentication procedures as commercial certificates; and we performed a system update to ensure those domains identified that were associated with mis-issuances cannot be used for new certificates without first undergoing standard authentication and issuance procedures.

Impacted WebTrust for CAs Criteria		Issues Noted
3	Principle 2, Criterion 7.2 requires that the CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	It was noted that physical access entry and exit logs for a Symantec CA facility were not archived for a minimum of 7 years as required by Criterion 7.2, the STN CPS and the Thawte CPS. 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 will be put in place to require supplemental approval and periodic monitoring of data retention requirements moving forward.
4	Principle 3, Criterion 8 requires that the CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals. Such controls must include, but are not limited to: • network security and firewall management, including port restrictions and IP address filtering and • logical access controls, activity logging (WTCA 2.0 Section 3.10), and inactivity time-outs to provide individual accountability.	It was noted that access to the CA applications to issue production certificates was not restricted only to authorized members of the Certificate Authentication Services team, but also included other Symantec employees for testing purposes. This additional access was used for application testing purposes. We completed a review of issuance privileges to confirm that only authorized personnel have the ability to issue certificates; we updated the rules regarding granting of privileges; and we have deployed an enhanced quarterly access review process to confirm the appropriateness of this access ongoing.

Impacted WebTrust for CAs Criteria		Issues Noted
5	Principle 4, Criterion 3 requires that the CA maintains controls to provide reasonable assurance that: • Certificate Systems under the control of CA capable of monitoring and logging system activity and are configured to continuously monitor and log system activity; • Automated mechanisms under the control of CA are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events; • Trusted Role personnel follows up on alerts of possible Critical Security Events; • A human review of application and system logs is performed at least every 30 days and includes: o Validating the integrity of logging processes o Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly; and • Maintain, archive, and retain logs in accordance with disclosed business practices.	It was noted that although logging was in place for selected in-scope systems, a process for periodically validating the integrity and effectiveness of the process, whereby a human review of application and system logs is performed at least every 30 days in accordance with CA Browser Forum Network Security requirements, was not in place during the examination period. Symantec has since put in place controls to continuously check for the presence of system monitoring processes. In addition, a bi-weekly audit process has been instituted to perform log-integrity verification.

Symantec Corporation

Roxane Divol
Senior Vice President of Trust Services

APPENDIX A – STN and Thawte SSL CAs

Symantec Root CAs:

- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Authorized Code Signing Root CA for Microsoft
- VeriSign Universal Root Certification Authority
- Symantec Class 1 Public Primary Certification Authority - G4
- Symantec Class 2 Public Primary Certification Authority - G4
- Symantec Class 3 Public Primary Certification Authority - G4
- Symantec Class 1 Public Primary Certification Authority - G6
- Symantec Class 2 Public Primary Certification Authority - G6
- Symantec Class 3 Public Primary Certification Authority - G6
- Symantec Class 1 Public Primary Certification Authority - G7
- Symantec Class 2 Public Primary Certification Authority - G7
- Symantec Class 3 Public Primary Certification Authority - G7

Thawte Root CAs:

- thawte Primary Root CA
- thawte Primary Root CA - G2
- thawte Primary Root CA - G3
- thawte Primary Root CA - G4

Symantec SSL Issuing CAs:

- VeriSign Class 3 International Server CA - G3
- VeriSign Class 3 Secure Server CA – G3
- VeriSign Class 3 Secure Server CA - T1
- VeriSign Class 3 International Server CA - T1
- Symantec Class 3 Secure Server CA - G4
- Symantec Class 3 DSA SSL CA
- Symantec Class 3 ECC 256 bit SSL CA
- Symantec Class 3 Secure Server SHA256 SSL CA
- Symantec Class 3 ECC 256 bit SSL CA - G2
- VeriSign Class 3 Extended Validation SSL CA
- VeriSign Class 3 Extended Validation SSL SGC CA
- VeriSign Class 3 Extended Validation CA - T1
- VeriSign Class 3 Extended Validation SGC CA - T1
- Symantec Class 3 DSA EV SSL CA
- Symantec Class 3 ECC 256 bit Extended Validation CA
- Symantec Class 3 EV SSL CA - G2
- Symantec Class 3 EV SSL CA - G3
- Symantec Class 3 EV SSL SGC CA - G2
- Symantec Class 3 Extended Validation SHA256 SSL CA
- Symantec Class 3 ECC 256 bit EV CA - G2

Thawte SSL Issuing CAs:

- Thawte SSL CA
- Thawte DV SSL CA
- Thawte SGC CA - G2
- thawte SSL CA - G2
- Thawte DSA CA
- Thawte SHA256 SSL CA
- thawte DV SSL SHA256 CA
- thawte DV SSL CA - G2
- Thawte Extended Validation SSL CA
- thawte EV SSL CA - G2
- thawte EV SSL CA - G3
- Thawte Extended Validation SHA256 SSL CA

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