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 Thawte Certification Authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; and Dublin, Ireland, regarding the disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, 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 its Thawte Symantec CAs listed in Appendix A.

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'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 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 Thawte CPS. This caused WebTrust for CAs Criterion 2.2 to not be met.
3.6	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.	During our examination, we 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 caused WebTrust for CAs Criterion 3.6 to not be met with respect to CA applications.
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 Thawte 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.

Impacted WebTrust for CAs Criteria		Issues Noted
6.1, 6.2, 6.3, and 6.4	The CA maintains control to provide reasonable assurance that: • For authenticated certificates, Subscribers are accurately identified in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate, authorized and complete. For domain validated certificates, Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate and complete. • Certificate rekey requests following certificate revocation or expiration are accurate, authorized and complete. • Certificate renewal requests are accurate, authorized and complete. • Certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorized and complete. • Certificates are generated and issued in accordance with the CA's disclosed business practices.	During our examination, we noted that 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 Criteria 6.1, 6.2, 6.3, and 6.4 to not be met.

In our opinion, except for the matters described in the preceding paragraphs, in providing its Symantec CA services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; and Dublin, Ireland 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 Thawte Certification Practice Statement ("CPS"), Version 3.7.14, dated September 24, 2015 ("Thawte CPS") on Symantec's Thawte website

- Symantec maintained effective controls to provide reasonable assurance that Symantec provided its services in accordance with its Certification Practice Statement

- Symantec maintained effective controls to provide reasonable assurance that:
  - the integrity of 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

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

- 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

APPENDIX A – Thawte Root and Issuing CAs

Thawte Root CAs:	**Thawte SSL Issuing CAs:**
• thawte Primary Root CA • thawte Primary Root CA - G2 • thawte Primary Root CA - G3 • thawte Primary Root CA - G4 • Thawte TimeStamping CA	• 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 **Thawte other Issuing CAs:** • Thawte Code Signing CA – G2 • thawte SHA256 Code Signing CA thawte SHA256 Code Signing CA - G2

Assertion by Management as to
its Disclosure of its Business Practices and its Controls
over Certification Authority Operations
during the Period from December 1, 2014 through November 30, 2015

May 13, 2016

Symantec Corporation ("Symantec") operates various Thawte Root and Issuing certification authorities (collectively referred to as the "Thawte CAs") that are listed in Appendix A and that provide the following range of CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key management

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

Management has assessed the controls over its Thawte CA operations. Based on that assessment, in Management's opinion, in providing its Certification Authority (CA) services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Cape Town, South Africa 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 Thawte Certification Practice Statement, Version 3.7.14, dated September 24, 2015 on the Symantec Thawte website

- Symantec maintained effective controls to provide reasonable assurance that Symantec provided its services in accordance with its Certification Practice Statement

- Symantec maintained effective controls to provide reasonable assurance that:
    - the integrity of 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 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)

CA Business Practices Management

- Certification Practice Management

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
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation

- Certificate Validation

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 Thawte CPS. HR has performed a validation of personnel requiring Trusted Status and 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.
3.6	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.	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
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.

Impacted WebTrust for CAs Criteria		Issues Noted
6.1, 6.2, 6.3, and 6.4	The CA maintains control to provide reasonable assurance that: • For authenticated certificates, Subscribers are accurately identified in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate, authorized and complete. For domain validated certificates, Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate and complete. • Certificate rekey requests following certificate revocation or expiration are accurate, authorized and complete. • Certificate renewal requests are accurate, authorized and complete. • Certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorized and complete. • Certificates are generated and issued in accordance with the CA's disclosed business practices.	It was noted that the 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 testing to unregistered domains. As we disclosed in our published incident reports, Symantec has completed a thorough investigation of its test certificates. Symantec's investigation uncovered no evidence of malicious intent, nor inappropriate use of these certificates. Each of these test certificates was issued solely for internal Symantec testing purposes that have since been revoked or have expired. Symantec contacted the relevant domain owners 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.

Symantec Corporation

Roxane Divol

Senior VP of Trust Services

APPENDIX A – Thawte Root and Issuing CAs

Thawte Root CAs:	**Thawte SSL Issuing CAs:**
• thawte Primary Root CA • thawte Primary Root CA - G2 • thawte Primary Root CA - G3 • thawte Primary Root CA - G4 • Thawte TimeStamping CA	• 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 **Thawte other Issuing CAs:** • Thawte Code Signing CA – G2 • thawte SHA256 Code Signing CA thawte SHA256 Code Signing CA - G2

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 v2.0 including the following:

CA Environmental Controls

- Physical and Environmental Security

Verisign, Inc.

Joseph David Pool

Senior Vice President of Architecture & Tech Services