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 for Symantec Corporation's ("Symantec") certification authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, and Verisign, Inc. ("Verisign"), an independent service organization that provides data center hosting services to Symantec, Symantec's disclosure of its SSL certificate life cycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Symantec website, the provision of such services in accordance with its disclosed practices, and the design of its controls over key and SSL certificate integrity, over the authenticity and confidentiality of SSL subscriber and relying party information, over continuity of key and SSL certificate life cycle management operations, and over development, maintenance, and operation of CA systems integrity, and over meeting the network and certificate system security requirements set forth by the CA/Browser Forum, throughout the period December 1, 2015 to June 15, 2016 for the GeoTrust CAs listed in Appendix A ("the GeoTrust Root and SSL Issuing CAs") in scope for SSL Baseline Requirements and Network Security Requirements.

These disclosures and controls are the responsibility of Symantec and Verisign's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0, based on our examination.

Symantec makes use of external registration authorities ("Affiliates") for specific subscriber registration activities as disclosed in the GeoTrust CPS. Our examination did not extend to the controls exercised by these external registration authorities.

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 SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Symantec's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management 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 matters that resulted in a modification of our opinion:

Impacted WebTrust for CAs Criteria		Matters Noted
1	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 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.
2	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 one of the CA facilities were not archived for 7 years as required by Criterion 7.2, and the GeoTrust 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.
3	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 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 access.

Impacted WebTrust for CAs Criteria		Matters Noted
4	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 in-scope systems selected for testing, 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.
5	Principle 4, Criterion 4 requires that the CA maintains controls to provide reasonable assurance that: • A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; • Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: o Within one week of receiving a request from the CA/Browser Forum, o After any system or network changes that the CA determines are significant, and o At least once per quarter; • Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant; • Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools,	The following was noted pertaining to in-scope systems for one international production environment (where two in-scope CAs are hosted): • vulnerability scans on internal IP addresses did not include all production systems in-scope • vulnerability scans on internal IP addresses were not consistently performed at least quarterly per the frequency requirements in the Network Security Requirements • a penetration test was not performed during the examination period.

Impacted WebTrust for CAs Criteria		Matters Noted
	proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; • Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: o Remediate the Critical Vulnerability; o If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: ▪ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ▪ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or o Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: ▪ The CA disagrees with the NVD rating; ▪ The identification is a false positive; ▪ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or ▪ Other similar reasons. (See Network and Certificate Systems Security Requirements Section 4)	

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, throughout the period December 1, 2015 to June 15, 2016, in all material respects:

- Symantec disclosed its SSL certificate life cycle management business practices in its GeoTrust Certification Practice Statement, Version 1.1.18 dated, September 24, 2015 ("GeoTrust CPS") including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Symantec website, and provided such services in accordance with its disclosed practices

- Symantec maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

- 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

- Symantec maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 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 – SSL Baseline with Network Security 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
February 28, 2017

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

APPENDIX A – GeoTrust Root and SSL Issuing CAs

GeoTrust Root CAs:	GeoTrust SSL Issuing CAs:
• GeoTrust Global CA • GeoTrust Primary Certification Authority • GeoTrust Primary Certification Authority - G2 • GeoTrust Primary Certification Authority - G3 • GeoTrust Primary Certification Authority - G4 • GeoTrust Universal CA • GeoTrust Universal CA 2 • GeoTrust Global CA 2	• GeoTrust Extended Validation SSL CA • GeoTrust Extended Validation SSL CA - G2 • GeoTrust EV SSL CA - G4 • GeoTrust Extended Validation SHA256 SSL CA • GeoTrust EV SSL CA - G5 • GeoTrust ECC EV SSL CA • GeoTrust SSL CA • GeoTrust DV SSL CA • RapidSSL CA • GeoTrust SSL CA - G2 • RapidSSL Enterprise CA • GeoTrust DV SSL CA - G2 • RapidSSL CA - G2 • GeoTrust SHA256 SSL CA • GeoTrust DSA SSL CA • GeoTrust SSL CA - G3 • RapidSSL Enterprise DSA SSL CA • RapidSSL SHA256 CA • GeoTrust DV SSL SHA256 CA • RapidSSL SHA256 CA - G2 • GeoTrust DV SSL CA - G3 • GeoTrust DV SSL CA - G4 • RapidSSL SHA256 CA - G3 • GeoTrust SSL CA - G4 • GeoTrust DV SSL SHA256 CA - G2 • RapidSSL SHA256 CA - G4 • GeoTrust Secure Site Starter DV SSL CA - G1 • Secure Site Starter DV SSL CA - G2 • Secure Site Starter DV SSL CA - G3 • Volusion, Inc. DV SSL CA • Volusion, Inc. DV SSL CA - G2 • Volusion, Inc. DV SSL CA - G3 • Intermediate Certificate DV SSL CA • Intermediate Certificate DV SSL CA - G2 • Intermediate Certificate DV SSL CA - G3 • STRATO SSL • STRATO SSL - G2 • STRATO SSL - G3 • Hostpoint DV SSL CA – G1 • Hostpoint DV SSL CA – G2 • Trust Provider B.V. DV SSL CA - G1 • Trust Provider B.V. DV SSL CA - G2 • AlwaysOnSSL CA - G1 • AlwaysOnSSL CA - G2 • TrustAsia Technologies, Inc. DV SSL CA - G1 • TrustAsia Technologies, Inc. DV SSL CA - G2 • STRATO SSL - G4 • STRATO SSL - G5 • Volusion, Inc. DV SSL CA - G4 • Volusion, Inc. DV SSL CA - G5 • DKHS Device CA • DKHS Device CA - G2

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, 2015 through June 15, 2016

February 28, 2017

Symantec Corporation ("Symantec") provides its GeoTrust SSL certification authority (CA) services through the GeoTrust CAs listed in Appendix A ("the GeoTrust Root and SSL Issuing CAs") in scope for SSL Baseline Requirements and Network Security Requirements.

Symantec also makes use of external registration authorities ("Affiliates") for specific subscriber registration activities as disclosed in the GeoTrust CPS.

The management of Symantec is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key life cycle management controls, and SSL certificate life cycle 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 Symantec's certification authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Symantec management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in Symantec management's opinion, in providing its SSL certification authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Cape Town, South Africa; Melbourne, Australia; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, throughout the period December 1, 2015 to June 15, 2016, Symantec has:

- disclosed its SSL certificate life cycle management business practices in its GeoTrust Certification Practice Statement, Version 1.1.18 dated, September 24, 2015 ("GeoTrust CPS") including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Symantec website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by 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

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0 except for the matters noted below.

Impacted WebTrust for CAs Criteria		Matters Noted
1	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 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		Matters Noted
2	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 one of the CA facilities were not archived for a minimum of 7 years as required by Criterion 7.2, and the GeoTrust 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.
3	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. As of June 15, 2016, 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		Matters Noted
4	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 in-scope systems selected for testing, 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.
5	Principle 4, Criterion 4 requires that the CA maintains controls to provide reasonable assurance that: • A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; • Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: o Within one week of receiving a request from the CA/Browser Forum, o After any system or network changes that the CA determines are significant, and o At least once per quarter;	The following was noted pertaining to in-scope systems for one international production environment (where two in-scope CAs are hosted): • vulnerability scans on internal IP addresses did not include all production systems in-scope • vulnerability scans on internal IP addresses were not consistently performed at least quarterly per the frequency requirements in the Network Security Requirements • a penetration test was not performed during the examination period. In addition to the external vulnerability scans already performed, Symantec has expanded its quarterly scan process to include the internal production hosts in the international location referenced above and a penetration test has been scheduled to complete in March 2017.

	• Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant; • Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; • Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: o Remediate the Critical Vulnerability; o If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: ▪ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ▪ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or o Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: ▪ The CA disagrees with the NVD rating; ▪ The identification is a false positive; ▪ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or ▪ Other similar reasons.	

Impacted WebTrust for CAs Criteria		Matters Noted
	(See Network and Certificate Systems Security Requirements Section 4)	

Symantec Corporation

Roxane Divol
EVP and GM, Website Security

APPENDIX A –GeoTrust Root and SSL Issuing CAs

GeoTrust Root CAs:	GeoTrust SSL Issuing CAs:
• GeoTrust Global CA • GeoTrust Primary Certification Authority • GeoTrust Primary Certification Authority - G2 • GeoTrust Primary Certification Authority - G3 • GeoTrust Primary Certification Authority - G4 • GeoTrust Universal CA • GeoTrust Universal CA 2 • GeoTrust Global CA 2	• GeoTrust Extended Validation SSL CA • GeoTrust Extended Validation SSL CA - G2 • GeoTrust EV SSL CA - G4 • GeoTrust Extended Validation SHA256 SSL CA • GeoTrust EV SSL CA - G5 • GeoTrust ECC EV SSL CA • GeoTrust SSL CA • GeoTrust DV SSL CA • RapidSSL CA • GeoTrust SSL CA - G2 • RapidSSL Enterprise CA • GeoTrust DV SSL CA - G2 • RapidSSL CA - G2 • GeoTrust SHA256 SSL CA • GeoTrust DSA SSL CA • GeoTrust SSL CA - G3 • RapidSSL Enterprise DSA SSL CA • RapidSSL SHA256 CA • GeoTrust DV SSL SHA256 CA • RapidSSL SHA256 CA - G2 • GeoTrust DV SSL CA - G3 • GeoTrust DV SSL CA - G4 • RapidSSL SHA256 CA - G3 • GeoTrust SSL CA - G4 • GeoTrust DV SSL SHA256 CA - G2 • RapidSSL SHA256 CA - G4 • GeoTrust Secure Site Starter DV SSL CA - G1 • Secure Site Starter DV SSL CA - G2 • Secure Site Starter DV SSL CA - G3 • Volusion, Inc. DV SSL CA • Volusion, Inc. DV SSL CA - G2 • Volusion, Inc. DV SSL CA - G3 • Intermediate Certificate DV SSL CA • Intermediate Certificate DV SSL CA - G2 • Intermediate Certificate DV SSL CA - G3 • STRATO SSL • STRATO SSL - G2 • STRATO SSL - G3 • Hostpoint DV SSL CA – G1 • Hostpoint DV SSL CA – G2 • Trust Provider B.V. DV SSL CA - G1 • Trust Provider B.V. DV SSL CA - G2 • AlwaysOnSSL CA - G1 • AlwaysOnSSL CA - G2 • TrustAsia Technologies, Inc. DV SSL CA - G1 • TrustAsia Technologies, Inc. DV SSL CA - G2 • STRATO SSL - G4 • STRATO SSL - G5 • Volusion, Inc. DV SSL CA - G4 • Volusion, Inc. DV SSL CA - G5 • DKHS Device CA • DKHS Device CA - G2

VERISIGN

Assertion by Management of Verisign, Inc.
Regarding its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
During the Period December 1, 2015 through June 15, 2016

February 28, 2017

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, 2015 through June 15, 2016, 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