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; 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 June 16, 2016 to November 30, 2016 for the Symantec CAs listed in Appendix A ("the Symantec STN 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 Symantec Trust Network (STN) Certification Practice Statement (CPS). Our examination did not extend to the controls exercised by these Affiliates.

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 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 in accordance with the Baseline Requirements 9.2.6 and STN CPS section 3.2.2, Symantec performed a review of SSL certificates with internal names, expiring after October 1, 2016. Although Symantec identified and revoked the majority of such certificates as part of this activity, in limited circumstances certificates with internal names with pending TLD status were not identified and revoked in a timely manner. These certificates have since been revoked. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 2, Criterion 2.2 to not be met.

Impacted WebTrust for CAs Criteria		Matters Noted
2	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 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)	It was noted that Symantec did not consistently maintain formal documentation of the basis for Symantec's determination that remediation was not required for critical vulnerabilities not requiring remediation, as required by WTBR criterion 4.4 and Symantec's Threat and Vulnerability Management Policy. This caused WebTrust for CAs – SSL Baseline with Network Security Principle 4, Criterion 4 to not be met.

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, throughout the period June 16, 2016 to November 30, 2016, in all material respects:

- Symantec disclosed its SSL certificate life cycle management business practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.24 dated September 9, 2016 ("STN CPS"); and Symantec Trust Network Certificate Policy, Version 2.8.20, dated September 9, 2016 ("STN CP") 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

for the Symantec Root and SSL Issuing CAs based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0.

Other Matter

It was noted that Symantec disclosed the issuance of 23 SHA-1 subscriber certificates, signed by the Verisign Class 3 International Server CA - G3 CA and Verisign Class 3 Secure Server CA – G3, in order to meet specific customer technical requirements. These certificates were issued as part of a formal SHA-1 application exception process after consultation with the CA/Browser Forum members as the current version of the CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("CABF Baseline Requirements") does not permit the issuance of SHA-1 certificates effective January 1, 2016. While issuance of a SHA-1 certificate is not permitted as per the current version of the CABF Baseline Requirements, there is no corresponding criterion in the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0 standard. Hence, our opinion is not modified with respect to this matter.

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 – Symantec STN Root and SSL Issuing CAs

Symantec Root CAs:	**Symantec SSL Issuing CAs:**
• VeriSign Class 3 Public Primary Certification Authority - G3 • VeriSign Class 3 Public Primary Certification Authority - G5 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Universal Root Certification Authority • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G4 • Symantec Class 3 Public Primary Certification Authority - G7	• VeriSign Class 3 Secure Server CA - G2 • 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 ECC 384 bit SSL CA • Symantec Class 3 Secure Server SHA256 SSL CA • Symantec Class 3 ECC 256 bit SSL CA - G2 • Symantec Basic DV SSL CA - G1 • Symantec Basic DV SSL CA - G2 • TrustAsia DV SSL CA - G5 • TrustAsia DV SSL CA - G6 • Oracle SSL CA • Oracle SSL CA - G2 • Wells Fargo Certificate Authority WS1 • Blue Coat Public Services Intermediate CA • 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 ECC 384 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 • Symantec Class 3 ECC 256 bit EV CA - G3 • Symantec Class 3 EV SSL CA - G4

Assertion of Management as to
Its Disclosure of its Business Practices and its Controls
Over its Certification Authority Operations
During the period from June 16, 2016 through November 30, 2016

February 28, 2017

Symantec Corporation ("Symantec") provides its Symantec certification authority (CA) services through the Symantec Trust Network (STN) CAs listed in Appendix A ("the Symantec STN 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 Symantec Trust Network (STN) Certification Practice Statement (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; and Kawasaki-shi, Japan, throughout the period June 16, 2016 to November 30, 2016, Symantec has:

- disclosed its SSL certificate life cycle management business practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.26 dated September 9, 2016 ("STN CPS") and Symantec Trust Network Certificate Policy, Version 2.8.22, dated September 9, 2016 ("STN CP") 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 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 in accordance with the Baseline Requirements 9.2.6 and STN CPS section 3.2.2, Symantec performed a review of SSL certificates with internal names, expiring after October 1, 2016. Although Symantec identified and revoked the majority of such certificates as part of this activity, in limited circumstances certificates with internal names with pending TLD status were not identified and revoked in a timely manner. These certificates have since been revoked. Prior to the October 1, 2016 change in Baseline Requirements regarding internal names, Symantec conducted an analysis in which we examined every CN and SAN in certificates still valid at the time. Following this analysis, Symantec identified and revoked the still valid certificates including internal names. We subsequently identified an edge case where certificates with internal names where the TLD status was pending with ICANN had not been included in our effort prior to the October 1, 2016 change. Once we identified this case, we revoked these remaining certificates using internal names. We publicly disclosed this issue and remediation when it occurred.

Impacted WebTrust for CAs Criteria		Matters Noted
2	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 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)	It was noted that Symantec did not consistently maintain formal documentation of the basis for Symantec's determination that remediation was not required for critical vulnerabilities not requiring remediation, as required by WTBR criterion 4.4 and Symantec's Threat and Vulnerability Management Policy. Symantec has updated its vulnerability management program to ensure that the disposition and associated analysis are consistently documented.

Symantec Corporation

Roxane Divol
EVP and GM, Website Security

APPENDIX A – Symantec STN Root and SSL Issuing CAs

Symantec Root CAs:	Symantec SSL Issuing CAs:
• VeriSign Class 3 Public Primary Certification Authority - G3 • VeriSign Class 3 Public Primary Certification Authority - G5 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Universal Root Certification Authority • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G4 • Symantec Class 3 Public Primary Certification Authority - G7	• VeriSign Class 3 Secure Server CA - G2 • 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 ECC 384 bit SSL CA • Symantec Class 3 Secure Server SHA256 SSL CA • Symantec Class 3 ECC 256 bit SSL CA - G2 • Symantec Basic DV SSL CA - G1 • Symantec Basic DV SSL CA - G2 • TrustAsia DV SSL CA - G5 • TrustAsia DV SSL CA - G6 • Oracle SSL CA • Oracle SSL CA - G2 • Wells Fargo Certificate Authority WS1 • Blue Coat Public Services Intermediate CA • 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 ECC 384 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 • Symantec Class 3 ECC 256 bit EV CA - G3 • Symantec Class 3 EV SSL CA - G4

VERISIGN

Assertion by Management of Verisign, Inc.
Regarding its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
During the Period June 16, 2016 through November 30, 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 June 16, 2016 through November 30, 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