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"), regarding the disclosure of its key and certificate life cycle management business practices, the effectiveness of its controls over key and SSL certificate integrity and the authenticity of subscriber information, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – V 1.4.5, during the period December 1, 2014 through November 30, 2015, for the Symantec owned GeoTrust Extended Validation SSL CAs (GeoTrust EV SSL CAs) in Appendix A.

Symantec's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion 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 (1) obtaining an understanding of Symantec's GeoTrust EV SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal and revocation of Symantec's GeoTrust EV SSL certificates; (2) selectively testing transactions executed in accordance with disclosed EV certificate life cycle 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 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'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
1	**Verification of Applicant** Principle 2, Criterion 13 requires that the CA maintains controls and procedures to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by only using at least one of the following verification methods: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; 2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at -sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; **Verification of EV SSL Certificate requests** Principle 2, Criterion 18 require that in cases where an EV SSL Certificate Request is submitted by a Certificate Requester, the CA maintains controls to provide reasonable assurance that, before it issues the requested EV SSL Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request.	During our examination, we noted that GeoTrust Issuing EV 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 Principles and Criteria for Certification Authorities – Extended Validation SSL V 1.4.5 Principle 2, Criteria 13 and 18 to not be met.
2	Principle 2, Criterion 49 requires that the CA and RA maintain controls to provide reasonable assurance that event logs at the CA and RA site 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 specified in the GeoTrust CPS. This caused WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V 1.4.5 Principle 2, Criterion 49, to not be met with respect to the retention of CA facility entry and exit logs.

In our opinion, except for the effects of the matter discussed in the preceding paragraphs, in providing its GeoTrust EV SSL CA services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, during the period December 1, 2014 through November 30, 2015, management of Symantec:

- Disclosed its GeoTrust EV SSL certificate practices and procedures in its GeoTrust Certification Practice Statement ("CPS"), Version 1.1.18, dated September 24, 2015 ("GeoTrust CPS"), including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines on the Symantec GeoTrust website and provided such services in accordance with its disclosed practices and
- Maintained effective controls to provide reasonable assurance that
  - EV subscriber information was properly collected, authenticated (for the registration activities performed by Symantec) and verified; and
  - The integrity of keys and EV certificates it manages was established and protected throughout their life cycles

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – V 1.4.5 for the GeoTrust EV SSL CAs.

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 – Extended Validation SSL – V 1.4.5, 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 – GeoTrust EV SSL CAs

GeoTrust EV SSL Root CAs:	**GeoTrust EV SSL Issuing CAs:**
• GeoTrust Primary Certification Authority • GeoTrust Primary Certification Authority - G2 • GeoTrust Primary Certification Authority - G3 • GeoTrust Primary Certification Authority - G4	• 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

Assertion of Management as to
Its Disclosure of its Business Practices and its Controls
Over its Extended Validation Certification Authority Operations
During the period from December 1, 2014 through November 30, 2015

May 13, 2016

Symantec Corporation ("Symantec") provides Extended Validation Certification Authority (EV-CA) services through the Symantec owned GeoTrust EV SSL CAs in Appendix A.

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

- Disclosed its GeoTrust EV SSL certificate practices and procedures in its GeoTrust Certification Practice Statement ("CPS"), Version 1.1.18, dated September 24, 2015 ("GeoTrust CPS"), including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines on the Symantec GeoTrust website and provided such services in accordance with its disclosed practices and
- Maintained effective controls to provide reasonable assurance that
  - EV subscriber information was properly collected, authenticated (for the registration activities performed by Symantec) and verified; and
  - The integrity of keys and EV certificates it manages was established and protected throughout their life cycles

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – V 1.4.5 except for the effects of the matters noted below:

Impacted WebTrust for CAs Criteria		Issues Noted
1	**Verification of Applicant** Principle 2, Criterion 13 requires that the CA maintains controls and procedures to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by only using at least one of the following verification methods: 5. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; 6. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 7. Communicating directly with the Domain Name Registrant using the contact information	It was noted that the GeoTrust Issuing EV 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. 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

Impacted WebTrust for CAs Criteria		Issues Noted
	listed in the WHOIS record's "registrant", "technical", or "administrative" field; 8. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at -sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; **Verification of EV SSL Certificate requests** Principle 2, Criterion 18 requires that in cases where an EV SSL Certificate Request is submitted by a Certificate Requester, the CA maintains controls to provide reasonable assurance that, before it issues the requested EV SSL Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request.	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.
2	Principle 2, Criterion 49 requires that the CA and RA maintain controls to provide reasonable assurance that event logs at the CA and RA site 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 specified in the CPS, to meet Principle 2, Criterion 49. Access log retention requirements for Symantec CA facilities exceed Symantec Corporate Security requirements. Due to recent personnel changes within the Corporate team that manages data retention across the company, CA facility log retention periods were reduced to match Corporate security log retention requirements without approval from the Symantec Website Security business unit. Upon identification and communication of the issue, the retention periods of physical access logs have since been updated to comply with the respective requirements for CA facilities. In addition, policy updates have been put in place to require supplemental approval and periodic monitoring of data retention requirements moving forward.

Symantec Corporation

Roxane Divol
Senior Vice President of Trust Services

APPENDIX A – GeoTrust EV SSL CAs

GeoTrust EV SSL Root CAs:	**GeoTrust EV SSL Issuing CAs:**
• GeoTrust Primary Certification Authority • GeoTrust Primary Certification Authority - G2 • GeoTrust Primary Certification Authority - G3 • GeoTrust Primary Certification Authority - G4	• 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