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 assertion 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 certificate integrity, and the authenticity of subscriber information, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – V 1.1, during the period December 1, 2014 through November 30, 2015, for its VeriSign Class 3 Public Primary Certification Authority – G5, Symantec Class 3 Extended Validation Code Signing CA, and Symantec Class 3 Extended Validation Code Signing CA - G2 CA (collectively referred to as the "STN EV CS CAs").

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 STN EV Code Signing certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of STN EV Code Signing certificates; (2) selectively testing transactions executed in accordance with disclosed STN EV Code Signing certificate lifecycle 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 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 issue that resulted in a modification of our opinion:

	Impacted WebTrust for CAs Criteria	Issue Noted
1	Principle 2, Criterion §59 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 STN CPS. This caused WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing V 1.1 Principle 2, Criterion 59, to not be met with respect to the retention of CA facility entry and exit logs.

In our opinion, except for the matter discussed above, in providing its Symantec STN EV CS services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, during the period to December 1, 2014 to November 30, 2015,

- Disclosed its STN EV Code Signing certificate practices and procedures in its Symantec Trust Network Certification Practice Statement, Version 3.8.21, dated November 25, 2015 ("STN CPS") and Symantec Certificate Policy, Version 2.8.17, dated November 30, 2015 ("STN CP"), including its commitment to provide EV Code Signing certificates in conformity with the applicable CA/Browser Forum Guidelines 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 Code Signing certificates it manages was established and protected throughout their lifecycles

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.1 for the STN EV 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 Code Signing v1.1, 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

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

May 13, 2016

Symantec Corporation ("Symantec") provides Extended Validation Code Signing Certification Authority (EV-CS) services through its VeriSign Class 3 Public Primary Certification Authority – G5, Symantec Class 3 Extended Validation Code Signing CA, and Symantec Class 3 Extended Validation Code Signing CA - G2 (collectively referred to as the "STN EV CS CAs").

Management has assessed its disclosures of its certificate practices and controls over its STN EV Code Signing CA services. Based on that assessment, in Symantec management's opinion, in providing its STN EV Code Signing Certification Authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan throughout the period from December 1, 2014 through November 30, 2015, Symantec has:

- Disclosed its STN EV Code Signing certificate practices and procedures in its Symantec Trust Network Certification Practice Statement, Version 3.8.21, dated November 25, 2015 ("STN CPS") and Symantec Certificate Policy, Version 2.8.17, dated November 30, 2015 ("STN CP"), including its commitment to provide EV Code Signing Certificates in conformity with the applicable CA/Browser Forum Guidelines 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 Code Signing certificates it manages was established and protected throughout their lifecycles

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.1 for the STN EV CAs, except for the effects of the matter noted below:

Impacted WebTrust for CAs Criteria		Issue Noted
1	Principle 2, Criterion §59 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 CA facility were not archived for a minimum of 7 years, as specified in the CPS, to meet Principle 2, Criterion 59. 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