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") for its Symantec Trust Network (STN) Extended Validation SSL ("EV SSL") certification authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; Cape Town, South Africa; and Kawasaki-shi, Japan, throughout the period June 16, 2016 to November 30, 2016 for its STN CAs listed in Appendix A ("the STN Root and EV SSL Issuing CAs"):

- Symantec disclosed its EV 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 EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates it manages is established and protected throughout their life cycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5.

Symantec's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion 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 EV SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
(2) selectively testing transactions executed in accordance with disclosed EV 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 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.

In our opinion, throughout the period June 16, 2016 to November 30, 2016, Symantec management's assertion, as referred to above, is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5

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 v1.4.5, nor the suitability of any of Symantec's services for any customer's intended purpose.

Symantec's use of the WebTrust for Certification Authorities – Extended Validation SSL Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

KPMG LLP

Certified Public Accountants
Santa Clara, CA
February 28, 2017

APPENDIX A –STN Root and EV SSL Issuing CAs

Symantec Root CAs:	**Symantec EV SSL Issuing CAs:**
• Symantec Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G5 • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G7 • VeriSign Universal Root Certification Authority	• 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 Extended Validation Certification Authority Operations
During the period from June 16, 2016 through November 30, 2016

February 28, 2017

Symantec Corporation ("Symantec") provides its Extended Validation SSL ("EV SSL") certification authority (CA) services through the Symantec Trust Network (STN) CAs listed in Appendix A (""the STN Root and EV SSL Issuing CAs").

The management of Symantec is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key life cycle management controls, and EV 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 EV SSL CA services. Based on that assessment, in Symantec management's opinion, in providing its EV SSL certification authority services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; Cape Town, South Africa; and Kawasaki-shi, Japan, throughout the period June 16, 2016 to November 30, 2016, Symantec has:

- disclosed its EV 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 EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates it manages is established and protected throughout their life cycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5.

Symantec Corporation

Roxane Divol
EVP and GM, Website Security

APPENDIX A –STN Root and EV SSL Issuing CAs

Symantec Root CAs:	Symantec EV SSL Issuing CAs:
• Symantec Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G5 • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G7 • VeriSign Universal Root Certification Authority	• 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