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") and Verisign, Inc. ("Verisign"), an independent service organization that provides data center hosting services to Symantec, for its 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, as of June 15, 2016 for its Symantec SSL CAs listed in Appendix A in scope for SSL Baseline Requirements and Network Security Requirements,

- Symantec disclosed its SSL certificate life cycle management business practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.24 dated May 20, 2016 ("STN CPS") and Symantec Trust Network Certificate Policy, Version 2.8.20, dated May 20, 2016 ("STN CP") including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the Symantec website, and provided such services in accordance with its disclosed practices
- Symantec suitably designed, and placed into operation, 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] suitably designed, and placed into operation, 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 suitably designed, and placed into operation, 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.

The management of Symantec and Verisign are responsible for their respective assertions. Our responsibility is to express an opinion on management assertions based on our examination.

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

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) evaluating the suitability of the design of the controls; and
(3) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Symantec's controls, individually or in the aggregate.

The suitability of the design of the 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 suitability of the design of the controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, the ability of Symantec and Verisign 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, as of June 15, 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 – SSL Baseline with Network Security v2.0.

Other Matter

During our examination, we noted that Symantec subsequently issued 18 SHA-1 subscriber certificates in July 2016, signed by the Verisign Class 3 International Server CA - G3 CA, 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, California
August 29, 2016

APPENDIX A – Symantec STN Root and SSL Issuing CAs

Symantec Root CAs:	**Symantec SSL Issuing CAs:**
• VeriSign Class 1 Public Primary Certification Authority - G3 • VeriSign Class 2 Public Primary Certification Authority - G3 • VeriSign Class 3 Public Primary Certification Authority - G3 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G5 • VeriSign Universal Root Certification Authority • Symantec Class 1 Public Primary Certification Authority - G4 • Symantec Class 2 Public Primary Certification Authority - G4 • Symantec Class 3 Public Primary Certification Authority - G4 • Symantec Class 1 Public Primary Certification Authority - G6 • Symantec Class 2 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 1 Public Primary Certification Authority - G7 • Symantec Class 2 Public Primary Certification Authority - G7 • Symantec Class 3 Public Primary Certification Authority - G7	• Symantec Class 3 DSA EV SSL CA • Symantec Class 3 DSA SSL CA • Symantec Class 3 ECC 256 bit EV CA - G2 • Symantec Class 3 ECC 256 bit EV CA - G3 • Symantec Class 3 ECC 256 bit Extended Validation CA • Symantec Class 3 ECC 256 bit SSL CA • Symantec Class 3 ECC 256 bit SSL CA - G2 • Symantec Class 3 ECC 384 bit Extended Validation CA • Symantec Class 3 ECC 384 bit SSL CA • Symantec Class 3 EV SSL CA - G2 • Symantec Class 3 EV SSL CA - G3 • Symantec Class 3 EV SSL CA - G4 • Symantec Class 3 EV SSL SGC CA - G2 • Symantec Class 3 Extended Validation SHA256 SSL CA • Symantec Class 3 Secure Server CA - G4 • Symantec Class 3 Secure Server SHA256 SSL CA • VeriSign Class 3 Extended Validation CA - T1 • VeriSign Class 3 Extended Validation SGC CA - T1 • VeriSign Class 3 Extended Validation SSL CA • VeriSign Class 3 Extended Validation SSL SGC CA • VeriSign Class 3 International Server CA - G3 • VeriSign Class 3 International Server CA - T1 • VeriSign Class 3 Secure Server CA - G3 • VeriSign Class 3 Secure Server CA - T1 • Blue Coat Public Services Intermediate CA • Oracle SSL CA • Oracle SSL CA - G2 • Wells Fargo Certificate Authority WS1

Assertion by Management as to
Its Disclosure of its Business Practices and its Controls
Over Certification Authority Operations
As of June 15, 2016

August 29, 2016

Symantec Corporation ("Symantec") provides Certification Authority (CA) services through the Symantec Trust Network (STN) SSL CAs listed in Appendix A in scope for SSL Baseline Requirements and Network Security Requirements.

The management of Symantec is responsible for establishing controls over its STN 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, controls placed into operation can only provide reasonable assurance with respect to Symantec's Certification Authority operations.

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; Melbourne, Australia; Cape Town, South Africa, Dublin, Ireland; and Kawasaki-shi, Japan, as of June 15, 2016,

- Symantec disclosed its SSL certificate life cycle management business practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.24 dated May 20, 2016 ("STN CPS") and Symantec Trust Network Certificate Policy, Version 2.8.20, dated May 20, 2016 ("STN CP") including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the Symantec website, and provided such services in accordance with its disclosed practices
- Symantec suitably designed, and placed into operation, 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 suitably designed, and placed into operation, 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 suitably designed, and placed into operation, 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.

Symantec Corporation

Roxane Divol
SVP and GM, Website Security

APPENDIX A – Symantec STN Root and SSL Issuing CAs

Symantec Root CAs:	Symantec SSL Issuing CAs:
• VeriSign Class 1 Public Primary Certification Authority - G3 • VeriSign Class 2 Public Primary Certification Authority - G3 • VeriSign Class 3 Public Primary Certification Authority - G3 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G5 • VeriSign Universal Root Certification Authority • Symantec Class 1 Public Primary Certification Authority - G4 • Symantec Class 2 Public Primary Certification Authority - G4 • Symantec Class 3 Public Primary Certification Authority - G4 • Symantec Class 1 Public Primary Certification Authority - G6 • Symantec Class 2 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 1 Public Primary Certification Authority - G7 • Symantec Class 2 Public Primary Certification Authority - G7 • Symantec Class 3 Public Primary Certification Authority - G7	• Symantec Class 3 DSA EV SSL CA • Symantec Class 3 DSA SSL CA • Symantec Class 3 ECC 256 bit EV CA - G2 • Symantec Class 3 ECC 256 bit EV CA - G3 • Symantec Class 3 ECC 256 bit Extended Validation CA • Symantec Class 3 ECC 256 bit SSL CA • Symantec Class 3 ECC 256 bit SSL CA - G2 • Symantec Class 3 ECC 384 bit Extended Validation CA • Symantec Class 3 ECC 384 bit SSL CA • Symantec Class 3 EV SSL CA - G2 • Symantec Class 3 EV SSL CA - G3 • Symantec Class 3 EV SSL CA - G4 • Symantec Class 3 EV SSL SGC CA - G2 • Symantec Class 3 Extended Validation SHA256 SSL CA • Symantec Class 3 Secure Server CA - G4 • Symantec Class 3 Secure Server SHA256 SSL CA • VeriSign Class 3 Extended Validation CA - T1 • VeriSign Class 3 Extended Validation SGC CA - T1 • VeriSign Class 3 Extended Validation SSL CA • VeriSign Class 3 Extended Validation SSL SGC CA • VeriSign Class 3 International Server CA - G3 • VeriSign Class 3 International Server CA - T1 • VeriSign Class 3 Secure Server CA - G3 • VeriSign Class 3 Secure Server CA - T1 • Blue Coat Public Services Intermediate CA • Oracle SSL CA • Oracle SSL CA - G2 • Wells Fargo Certificate Authority WS1

Assertion by Management of Verisign, Inc.
Regarding its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
As of June 15, 2016

August 29, 2016

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 placing in operation 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 as of June 15, 2016, Verisign has

- Suitably designed, and placed in operation, 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