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; and Dublin, Ireland, as of June 15, 2016 for its Thawte CAs listed in Appendix A,

- Symantec disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in its Thawte Certification Practice Statement, Version 3.7.15, dated March 8, 2016 ("Thawte CPS") on Symantec's Thawte website

- Symantec suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - Symantec provides its services in accordance with its Certification Practice Statement

- Symantec suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Symantec); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

based on the WebTrust Principles and Criteria for Certification Authorities 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.

The management of Symantec makes use of external registration ("Affiliates") authorities for specific subscriber registration activities as disclosed in Symantec's business practices. Our examination did not extend to the controls exercised by these affiliates.

[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 key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the logical and physical access to CA systems, over the continuity of key and certificate life cycle management operations and over development, maintenance and operation of systems integrity;
(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 v2.0.

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 v2.0, nor the suitability of any of Symantec's services for any customer's intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, Clalifornia
August 29, 2016

APPENDIX A – Symantec's Thawte Root and SSL Issuing CAs

Thawte Root CAs:	**Thawte SSL Issuing CAs:**
• thawte Primary Root CA • thawte Primary Root CA - G2 • thawte Primary Root CA - G3 • thawte Primary Root CA - G4	• thawte DSA SSL CA • Thawte DV SSL CA • thawte DV SSL CA - G2 • thawte DV SSL SHA256 CA • thawte ECC EV SSL CA • thawte EV SSL CA - G2 • thawte EV SSL CA - G3 • thawte Extended Validation SHA256 SSL CA • Thawte Extended Validation SSL CA • Thawte SGC CA - G2 • thawte SHA256 SSL CA • Thawte SSL CA • thawte SSL CA - G2

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") operates various Thawte Root and Issuing Certification Authorities (collectively referred to as the Thawte CAs) are listed in Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of Symantec is responsible for establishing controls over its Thawte CA operations, including its CA business practices disclosure in its Thawte CPS on its website, CA business practices management, CA environmental controls, CA key life cycle management controls, subscriber key life cycle management controls, certificate life cycle management controls, and subordinate CA 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 Thawte Certification Authority operations.

Management has assessed its disclosures of its certificate practices and controls over its Thawte CA services. Based on that assessment, in Symantec's management's opinion, in providing its Certification Authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Cape Town, South Africa, as of June 15, 2016,

- Symantec disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in its Thawte Certification Practice Statement, Version 3.7.15, dated March 8, 2016 ("Thawte CPS") on the Symantec Thawte website

- Symantec suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - Symantec provides its services in accordance with its Certification Practice Statement

- Symantec suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;

  - subscriber information is properly authenticated (for the registration activities performed by Symantec); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

based on the WebTrust Principles and Criteria for Certification Authorities v2.0, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Life cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls

- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey

- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

Symantec Corporation

Roxane Divol
SVP and GM Website Security

APPENDIX A – Symantec's Thawte Root and SSL Issuing CAs

Thawte Root CAs:	Thawte SSL Issuing CAs:
• thawte Primary Root CA • thawte Primary Root CA - G2 • thawte Primary Root CA - G3 • thawte Primary Root CA - G4	• thawte DSA SSL CA • Thawte DV SSL CA • thawte DV SSL CA - G2 • thawte DV SSL SHA256 CA • thawte ECC EV SSL CA • thawte EV SSL CA - G2 • thawte EV SSL CA - G3 • thawte Extended Validation SHA256 SSL CA • Thawte Extended Validation SSL CA • Thawte SGC CA - G2 • thawte SHA256 SSL CA • Thawte SSL CA • thawte SSL CA - G2

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 v2.0 including the following:

CA Environmental Controls

- Physical and Environmental Security

Verisign, Inc.

Joseph David Pool
Senior Vice President of Architecture & Tech Services