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 the Symantec 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, throughout the period June 16, 2016 to November 30, 2016 for the Symantec CAs listed in Appendix A ("the Symantec STN Root and Issuing CAs"):

- Symantec disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control 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") on the Symantec website

- Symantec maintained effective controls to provide reasonable assurance that:
  - Symantec's Certification Practice Statement is consistent with its Certificate Policy
  - Symantec provides its services in accordance with its Certificate Policy and Certification Practice Statement

- Symantec maintained effective 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] maintained effective 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's assertions, based on our examination.

The relative effectiveness and significance of specific controls at Symantec and Verisign 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. Our examination did not extend to

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

controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Symantec makes use of external registration authorities ("Affiliates") for specific subscriber registration activities as disclosed in Symantec Trust Network (STN) Certification Practice Statement (CPS). Our examination did not extend to the controls exercised by these Affiliates.

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 continuity of key and certificate life cycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and 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.

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 and Verisign management's assertions, as referred to above, are 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.

Symantec's use of the WebTrust for Certification Authorities 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 – Symantec STN Root and Issuing CAs

Symantec Root 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 - G5
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Universal Root Certification Authority
- 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 - G4
- Symantec Class 2 Public Primary Certification Authority - G4
- Symantec Class 3 Public Primary Certification Authority - G4
- 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 Internal Root CA

Symantec SSL Issuing CAs:

- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 International Server CA - G3
- VeriSign Class 3 Secure Server CA - G3
- VeriSign Class 3 Secure Server CA - T1
- VeriSign Class 3 International Server CA - T1
- Symantec Class 3 Secure Server CA - G4
- Symantec Class 3 DSA SSL CA
- Symantec Class 3 ECC 256 bit SSL CA
- Symantec Class 3 ECC 384 bit SSL CA
- Symantec Class 3 Secure Server SHA256 SSL CA
- Symantec Class 3 ECC 256 bit SSL CA - G2
- Symantec Basic DV SSL CA - G1
- Symantec Basic DV SSL CA - G2
- TrustAsia DV SSL CA - G5
- TrustAsia DV SSL CA - G6
- Oracle SSL CA
- Oracle SSL CA - G2
- Wells Fargo Certificate Authority WS1
- Blue Coat Public Services Intermediate CA
- 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

Symantec Other Issuing CAs:

- VeriSign Class 1 Individual Subscriber CA - G3
- VeriSign Class 2 MPKI Individual Subscriber CA - G2
- Symantec Class 1 Individual Subscriber CA - G4
- Symantec Class 1 Individual Subscriber CA - G5
- Symantec Class 2 Shared Intermediate Certificate Authority
- Symantec Class 2 Shared Intermediate Certificate Authority - G2
- Symantec Class 3 Organizational CA - G2
- Symantec Class 3 Organizational CA - G3
- Symantec Class 3 Organizational CA - G4
- Symantec Class 3 Organizational CA - G5
- VeriSign Class 3 Managed PKI Administrator CA - G3
- Symantec Class 3 Enterprise Service Center Admin CA
- Symantec Class 3 Shared Public Organization CA - SHA1
- Symantec Class 3 Shared Public Organization CA - SHA256

	• Symantec Class 3 Admin Intermediate Certificate Authority • Symantec Class 3 Registration Authority Intermediate CA • Symantec Class 3 Managed PKI Administrator CA - G4 • VeriSign Class 3 Code Signing 2010 CA • Symantec Class 3 SHA256 Code Signing CA • Symantec Class 3 SHA256 Code Signing CA - G2 • Symantec Class 3 Extended Validation Code Signing CA • Symantec Class 3 Extended Validation Code Signing CA - G2 • Symantec Class 3 Extended Validation Code Signing CA - G3 • Symantec SHA256 TimeStamping CA

Assertion by Management as to
Its Disclosure of its Business Practices and its Controls
Over Certification Authority Operations
During the Period from June 16, 2016 through November 30, 2016

February 28, 2017

Symantec Corporation ("Symantec") provides the following certification services through the Symantec CAs listed in Appendix A ("the Symantec STN Root and Issuing CAs"):

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

Symantec also makes use of external registration authorities ("Affiliates") for specific subscriber registration activities as disclosed in the Symantec Trust Network (STN) Certification Practice Statement (CPS).

The management of Symantec is responsible for establishing and maintaining effective controls over its STN CA operations, including its CA business practices disclosure in its STN CP and 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, even effective controls can only provide reasonable assurance with respect to Symantec and Verisign'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 CA services. Based on that assessment, in Symantec management's opinion, in providing its Symantec STN Root and Issuing CA services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; Cape Town, South Africa; and Kawasaki-shi, Japan, during the period June 16, 2016 to November 30, 2016, Symantec has:

- disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.26 dated September 9, 2016 and Symantec Trust Network Certificate Policy, Version 2.8.22, dated September 9, 2016

- maintained effective controls to provide reasonable assurance that:
  - Symantec's Certification Practice Statement is consistent with its Certificate Policy
  - Symantec provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective 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

- maintained effective 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)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

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
EVP and GM, Website Security

APPENDIX A – Symantec STN Root and Issuing CAs

Symantec Root 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 - G5
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Universal Root Certification Authority
- 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 - G4
- Symantec Class 2 Public Primary Certification Authority - G4
- Symantec Class 3 Public Primary Certification Authority - G4
- 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 Internal Root CA

Symantec SSL Issuing CAs:

- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 International Server CA - G3
- VeriSign Class 3 Secure Server CA - G3
- VeriSign Class 3 Secure Server CA - T1
- VeriSign Class 3 International Server CA - T1
- Symantec Class 3 Secure Server CA - G4
- Symantec Class 3 DSA SSL CA
- Symantec Class 3 ECC 256 bit SSL CA
- Symantec Class 3 ECC 384 bit SSL CA
- Symantec Class 3 Secure Server SHA256 SSL CA
- Symantec Class 3 ECC 256 bit SSL CA - G2
- Symantec Basic DV SSL CA - G1
- Symantec Basic DV SSL CA - G2
- TrustAsia DV SSL CA - G5
- TrustAsia DV SSL CA - G6
- Oracle SSL CA
- Oracle SSL CA - G2
- Wells Fargo Certificate Authority WS1
- Blue Coat Public Services Intermediate CA
- 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

Symantec Other Issuing CAs:

- VeriSign Class 1 Individual Subscriber CA - G3
- VeriSign Class 2 MPKI Individual Subscriber CA - G2
- Symantec Class 1 Individual Subscriber CA - G4
- Symantec Class 1 Individual Subscriber CA - G5
- Symantec Class 2 Shared Intermediate Certificate Authority
- Symantec Class 2 Shared Intermediate Certificate Authority - G2
- Symantec Class 3 Organizational CA - G2
- Symantec Class 3 Organizational CA - G3
- Symantec Class 3 Organizational CA - G4
- Symantec Class 3 Organizational CA - G5
- VeriSign Class 3 Managed PKI Administrator CA - G3
- Symantec Class 3 Enterprise Service Center Admin CA
- Symantec Class 3 Shared Public Organization CA - SHA1
- Symantec Class 3 Shared Public Organization CA - SHA256
- Symantec Class 3 Admin Intermediate Certificate Authority
- Symantec Class 3 Registration Authority Intermediate CA

	• Symantec Class 3 Managed PKI Administrator CA - G4 • VeriSign Class 3 Code Signing 2010 CA • Symantec Class 3 SHA256 Code Signing CA • Symantec Class 3 SHA256 Code Signing CA - G2 • Symantec Class 3 Extended Validation Code Signing CA • Symantec Class 3 Extended Validation Code Signing CA - G2 • Symantec Class 3 Extended Validation Code Signing CA - G3 • Symantec SHA256 TimeStamping CA

VERISIGN

Assertion by Management of Verisign, Inc.
Regarding its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
During the Period June 16, 2016 through November 30, 2016

February 28, 2017

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 maintaining effective 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 during the period June 16, 2016 through November 30, 2016, Verisign has

- Maintained effective 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