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 for Symantec Corporation's ("Symantec") certification authority (CA) operations at Mountain View, California and New Castle, Delaware, and Verisign, Inc. ("Verisign"), an independent service organization that provides data center hosting services to Symantec, Symantec's disclosure of its business, key life cycle management, certificate life cycle management, and CA environmental control practices, the provision of services in accordance with its Certification Practice Statement, and the effectiveness of its controls over key and certificate integrity, the authenticity and confidentiality of subscriber and relying party information, the continuity of key and certificate life cycle management operations, and development, maintenance, and operation of CA systems integrity throughout the period December 1, 2015 to June 15, 2016 for Symantec's WiMAX Forum ® Device Root CA1, WiMAX Forum ® Server Root CA2, and the WiMAX Forum ® Server Root CA3 (collectively referred to as the "Symantec WiMAX CAs").

These disclosures and controls are the responsibility of Symantec and Verisign's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities v2.0, based on our examination.

Symantec makes use of external registration authorities for specific subscriber registration activities for the Symantec WiMAX CAs as disclosed in the Symantec Certification Practices Statement for the WiMAX Forum ® Device PKI, Version 1.3, dated September 15, 2011 and the Symantec Certification Practices Statement for the WiMAX Forum ® Server PKI, Version 1.3 dated September 15, 2011 (collectively referred to as the "WiMAX CPS documents" and restricted to authorized users through the WiMAX Forum).

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.

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

We noted the following matters that resulted in a modification of our opinion:

	Impacted WebTrust for CAs Criteria	Matters Noted
1.1	The CA discloses its business practices including but not limited to the topics listed in RFC 3647, RFC 2527, or WebTrust for Certification Authorities v1 CA Business Practices Disclosure Criteria in its Certification Practice Statement.	It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the WiMAX CPS. This caused WebTrust for CAs Criterion 1.1 to not be met.
3.10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	It was noted that physical access entry and exit logs for one of the CA facilities were not archived for 7 years as specified in the WiMAX CPS. This caused WebTrust for CAs Criterion 3.10 to not be met with respect to the retention of CA facility entry and exit logs.

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, throughout the period December 1, 2015 to June 15, 2016, in all material respects:

- Symantec disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in the WiMAX CPS documents restricted to authorized users through the WiMAX Forum)

- Symantec maintained effective controls to provide reasonable assurance that:
  - Symantec provides its services in accordance with its Certification Practice Statements

- 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; and
  - subscriber information is properly authenticated (for the registration activities performed by Symantec)

- 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

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

for the Symantec WiMAX CAs based on the WebTrust Principles and Criteria for Certification Authorities v2.0.

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.

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, CA
February 28, 2017

Assertion by Management as to
Its Disclosure of its Business Practices and its Controls
Over Certification Authority Operations
During the Period from December 1, 2015 through June 15, 2016

February 28, 2017

Symantec Corporation ("Symantec") provides the following certification services through the WiMAX Forum ® Device Root CA1, WiMAX Forum ® Server Root CA2, and the WiMAX Forum ® Server Root CA3 (collectively referred to as the "Symantec WiMAX CAs"):

- Subscriber registration
- Certificate renewal (except for the WiMAX Forum ® Device Root CA1 which supports rekey but not renewal)
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

Symantec makes use of external registration authorities for specific subscriber registration activities for the Symantec WiMAX CAs as disclosed in the Symantec Certification Practices Statement for the WiMAX Forum ® Device PKI, Version 1.3, dated September 15, 2011 and the Symantec Certification Practices Statement for the WiMAX Forum ® Server PKI, Version 1.3 dated September 15, 2011 (collectively referred to as the "WiMAX CPS documents" and restricted to authorized users through the WiMAX Forum).

The management of Symantec is responsible for establishing and maintaining effective controls over its WiMAX CA operations, including its CA business practices disclosure in its WiMAX CPS documents, CA business practices management, CA environmental controls, CA key life cycle management controls, subscriber key life cycle management controls, and 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 WiMAX CA services. Based on that assessment, in Symantec management's opinion, in providing its WiMAX CA services at Mountain View, California and New Castle, Delaware throughout the period December 1, 2015 to June 15, 2016, Symantec has:

- disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in its WiMAX CPS documents restricted to authorized users through the WiMAX Forum

- maintained effective controls to provide reasonable assurance that:
  - Symantec provides its services in accordance with its Certification Practice Statements

- 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; and

  - subscriber information is properly authenticated (for the registration activities performed by Symantec)

- 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)

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

except for the effects of the matters noted below:

	Impacted WebTrust for CAs Criteria	Matters Noted
1.1	The CA discloses its business practices including but not limited to the topics listed in RFC 3647, RFC 2527, or WebTrust for Certification Authorities v1 CA Business Practices Disclosure Criteria in its Certification Practice Statement.	It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the CPS. HR has performed a validation of personnel requiring Trusted Status. Management also reiterated internal procedures to ensure that all reinvestigations are consistently performed.
3.10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	It was noted that physical access entry and exit logs for one of the CA facilities were not archived for a minimum of 7 years, as specified in the CPS, to meet Principle 3, Criterion 3.10. 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. The retention periods of physical access logs have 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
EVP and GM, Website Security

VERISIGN

Assertion by Management of Verisign, Inc.
Regarding its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
During the Period December 1, 2015 through June 15, 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 December 1, 2015 through June 15, 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 – 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