



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") Thawte certification authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; and Dublin, Ireland 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 its Thawte CAs listed in Appendix A (the "Thawte Root and Issuing 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 ("Affiliates") for specific subscriber registration activities as disclosed in the Thawte CPS. Our examination did not extend to the controls exercised by these external registration authorities.

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 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.	<p>It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the Thawte CPS.</p> <p>This caused WebTrust for CAs Criterion 1.1 to not be met.</p>
3.6	<p>The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that:</p> <ul style="list-style-type: none"><li>• Operating system and database access is limited to authorized individuals with predetermined task privileges;</li><li>• Access to network segments housing CA systems is limited to authorized individuals, applications and services; and</li><li>• CA application use is limited to authorized individuals.</li></ul>	<p>It was noted that access to the CA applications to issue production certificates was not restricted only to authorized members of the Certificate Authentication Services team but also included other Symantec employees for testing purposes.</p> <p>This caused WebTrust for CAs Criterion 3.6 to not be met with respect to CA applications access.</p>
3.10	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"><li>• significant CA environmental, key management, and certificate management events are accurately and appropriately logged;</li><li>• the confidentiality and integrity of current and archived audit logs are maintained;</li><li>• audit logs are completely and confidentially archived in accordance with disclosed business practices; and</li><li>• audit logs are reviewed periodically by authorized personnel.</li></ul>	<p>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 Thawte CPS.</p> <p>This caused WebTrust for CAs Criterion 3.10 to not be met with respect to the retention of CA facility entry and exit logs.</p>



	Impacted WebTrust for CAs Criteria	Matters Noted
6.1, 6.2, 6.3, and 6.4	<p>The CA maintains control to provide reasonable assurance that:</p> <ul style="list-style-type: none"><li>• For authenticated certificates, Subscribers are accurately identified in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate, authorized and complete. For domain validated certificates, Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate and complete.</li><li>• Certificate rekey requests following certificate revocation or expiration are accurate, authorized and complete.</li><li>• Certificate renewal requests are accurate, authorized and complete.</li><li>• Certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorized and complete.</li><li>• Certificates are generated and issued in accordance with the CA's disclosed business practices.</li></ul>	<p>It was noted that Issuing SSL CAs were used to issue certificates for Symantec internal testing purposes for registered domains that Symantec did not own. As required by the CPS, Symantec did not obtain the required authorization from the respective registered domain owners prior to certificate issuance. Furthermore, certificates were also issued for internal testing purposes to unregistered domains.</p> <p>This caused WebTrust Criteria 6.1, 6.2, 6.3, and 6.4 to not be met.</p>

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 its Thawte Certification Practice Statement, Version 3.7.15 dated, March 8, 2016 ("Thawte CPS") on Symantec's Thawte website
- Symantec maintained effective controls to provide reasonable assurance that Symantec provides its services in accordance with its 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<sup>1</sup> 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

<sup>1</sup> Limited to only physical access to CA systems and data hosted within the Verisign data center in New Castle, Delaware



Page 4

- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

for the Thawte Root and Issuing 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

**APPENDIX A –Thawte Root and Issuing CAs**

<p><b>Thawte Root CAs:</b></p> <ul style="list-style-type: none"><li>• Thawte Primary Root CA</li><li>• Thawte Primary Root CA - G2</li><li>• Thawte Primary Root CA - G3</li><li>• Thawte Primary Root CA - G4</li><li>• Thawte TimeStamping CA</li><li>• Symantec Time Stamping Services CA - G2</li></ul>	<p><b>Thawte SSL Issuing CAs:</b></p> <ul style="list-style-type: none"><li>• Thawte SSL CA</li><li>• Thawte DV SSL CA</li><li>• Thawte SGC CA - G2</li><li>• Thawte SSL CA - G2</li><li>• Thawte DSA SSL CA</li><li>• Thawte SHA256 SSL CA</li><li>• Thawte DV SSL SHA256 CA</li><li>• Thawte DV SSL CA - G2</li><li>• Thawte Extended Validation SSL CA</li><li>• Thawte EV SSL CA - G2</li><li>• Thawte EV SSL CA - G3</li><li>• Thawte Extended Validation SHA256 SSL CA</li><li>• Thawte ECC EV SSL CA</li></ul> <p><b>Thawte Other Issuing CAs:</b></p> <ul style="list-style-type: none"><li>• Thawte Code Signing CA - G2</li><li>• Thawte SHA256 Code Signing CA</li><li>• Thawte SHA256 Code Signing CA - G2</li><li>• Thawte EV Code Signing CA</li></ul>
--	--



**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 Thawte CAs listed in Appendix A ("the Thawte 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 Thawte CPS.

The management of Symantec is responsible for establishing and maintaining effective controls over its Symantec and Verisign CA operations, including its CA business practices disclosure in 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, 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 controls over its CA operations. Based on that assessment, in Symantec management's opinion, in providing its Thawte Root CA and Issuing CA services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; and Dublin, Ireland, , 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 Thawte Certification Practice Statement, Version 3.7.15 dated, March 8, 2016 ("Thawte CPS")
- maintained effective controls to provide reasonable assurance that Symantec provides its services in accordance with its 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)

#### **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

except for the effects of the matters noted below:

Impacted WebTrust for CAs Criteria		Matters Noted
1.1	<p>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.</p>	<p>It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the Thawte CPS.</p> <p>As of June 15, 2016, HR has performed a validation of personnel requiring Trusted Status. Management also reiterated internal procedures to ensure that all reinvestigations are consistently performed.</p>
3.6	<p>The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• Operating system and database access is limited to authorized individuals with predetermined task privileges;</li> <li>• Access to network segments housing CA systems is limited to authorized individuals, applications and services; and</li> <li>• CA application use is limited to authorized individuals.</li> </ul>	<p>It was noted that access to the CA applications to issue production certificates were not restricted only to authorized members of the Certificate Authentication Services team but also included other Symantec employees for testing purposes.</p> <p>This additional access was used for application testing purposes. As of June 15, 2016, we completed a review of issuance privileges to confirm that only authorized personnel have the ability to issue certificates; we updated the rules regarding granting of privileges; and we have deployed an enhanced quarterly access review process to confirm the appropriateness of this access ongoing.</p>



	Impacted WebTrust for CAs Criteria	Matters Noted
3.10	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• significant CA environmental, key management, and certificate management events are accurately and appropriately logged;</li> <li>• the confidentiality and integrity of current and archived audit logs are maintained;</li> <li>• audit logs are completely and confidentially archived in accordance with disclosed business practices; and</li> <li>• audit logs are reviewed periodically by authorized personnel.</li> </ul>	<p>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.</p> <p>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. Upon identification and communication of the issue, the retention periods of physical access logs have since 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.</p>

	Impacted WebTrust for CAs Criteria	Matters Noted
<p>6.1, 6.2, 6.3, and 6.4</p>	<p>The CA maintains control to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• For authenticated certificates, Subscribers are accurately identified in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate, authorized and complete. For domain validated certificates, Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and Subscriber's certificate requests are accurate and complete.</li> <li>• Certificate rekey requests following certificate revocation or expiration are accurate, authorized and complete.</li> <li>• Certificate renewal requests are accurate, authorized and complete.</li> <li>• Certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorized and complete.</li> <li>• Certificates are generated and issued in accordance with the CA's disclosed business practices.</li> </ul>	<p>It was noted that Issuing SSL CAs were used to issue certificates for Symantec internal testing purposes for registered domains that Symantec did not own. As required by the CPS, Symantec did not obtain the required authorization from the respective registered domain owners prior to certificate issuance. Furthermore, certificates were also issued for testing to unregistered domains.</p> <p>As we disclosed in our published incident reports, Symantec has completed a thorough investigation of its test certificates. Symantec's investigation uncovered no evidence of malicious intent, nor inappropriate use of these certificates. Each of these test certificates was issued solely for internal Symantec testing purposes that have since been revoked or have expired. Symantec contacted the relevant domain owners and provided relevant information to the browser community to enable the browsers to evaluate the appropriateness of blacklisting these test certificates where they deemed appropriate. We have also disabled access to technical features that enabled mis-issuance of test certificates; we updated our policies, internal procedures and trainings to clarify the April 2014 change in the Baseline Requirements that removed authorization to issue certificates to unregistered domains; we updated our internal policies, procedures and trainings to strongly reinforce that test certificates must follow the same authentication procedures as commercial certificates; and we performed a system update to ensure those domains identified that were associated with mis-issuances cannot be used for new certificates without first undergoing standard authentication and issuance procedures.</p>

Symantec Corporation

Roxane Divol  
EVP and GM, Website Security



**APPENDIX A –Thawte Root and Issuing CAs**

<p><b>Thawte Root CAs:</b></p> <ul style="list-style-type: none"><li>• thawte Primary Root CA</li><li>• thawte Primary Root CA - G2</li><li>• thawte Primary Root CA - G3</li><li>• thawte Primary Root CA - G4</li><li>• Thawte TimeStamping CA</li><li>• Symantec Time Stamping Services CA - G2</li></ul>	<p><b>Thawte SSL Issuing CAs:</b></p> <ul style="list-style-type: none"><li>• Thawte SSL CA</li><li>• Thawte DV SSL CA</li><li>• Thawte SGC CA - G2</li><li>• thawte SSL CA - G2</li><li>• thawte DSA SSL CA</li><li>• thawte SHA256 SSL CA</li><li>• thawte DV SSL SHA256 CA</li><li>• thawte DV SSL CA - G2</li><li>• thawte Extended Validation SSL CA</li><li>• thawte EV SSL CA - G2</li><li>• thawte EV SSL CA - G3</li><li>• thawte Extended Validation SHA256 SSL CA</li><li>• thawte ECC EV SSL CA</li></ul> <p><b>Thawte Other Issuing CAs:</b></p> <ul style="list-style-type: none"><li>• Thawte Code Signing CA - G2</li><li>• thawte SHA256 Code Signing CA</li><li>• thawte SHA256 Code Signing CA - G2</li><li>• thawte EV Code Signing CA</li></ul>
--	--



**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 v2.0 including the following:

**CA Environmental Controls**

- Physical and Environmental Security

Verisign, Inc.

A handwritten signature in black ink that reads "Joseph D. Pool".

Joseph David Pool  
Senior Vice President of Architecture & Tech Services