Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, #800
St. Louis, MO 63105

# REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Symantec Corporation:

We have examined for the Symantec Corporation's ("Symantec") Certification Authority ("CA") operations at Mountain View, California, USA and New Castle, Delaware, USA and for Verisign, Inc. ("Verisign"), an independent service organization that provides datacenter hosting services to Symantec at the New Castle, Delaware location:

a) Symantec's disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices and its disclosure of the services and related controls provided by Verisign in Attachment A; and

b) the effectiveness of Symantec's controls and Verisign's controls, where applicable, over the:
   - provision of services in accordance with its Symantec Managed PKI (MPKI) Adobe® Approved Trust List (AATL) Certification Practices Statement ("AATL CPS") and the description of the services and related controls provided by Verisign as enumerated in Attachment A,
   - establishment and protection of the integrity of keys and certificates it manages throughout their lifecycle,
   - authenticity and confidentiality of subscriber and relying party information,
   - continuity of key and certificate lifecycle management operations, and
   - development, maintenance, and operation of CA systems integrity

throughout the period December 1, 2016 to October 31, 2017 for its CAs as enumerated in Attachment B.

Symantec's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities v2.0. Our responsibility is to express an opinion 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 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 for specific subscriber registration activities as disclosed in the AATL CPS. Our examination did not extend to the controls exercised by these external registration authorities.

Symantec does not escrow its CA keys, and does not provide certificate renewal or suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period December 1, 2016 to October 31, 2017, for the CAs enumerated in Attachment B, in all material respects:

a) Symantec disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices for the services and related controls provided by Verisign in Attachment A; and

b) Symantec and Verisign, where applicable, maintained effective controls over the:
   - provision of services in accordance with its AATL CPS and the description of the services and related controls provided by Verisign as enumerated in Attachment A,
   - establishment and protection of the integrity of keys and certificates it manages throughout their lifecycle,
   - authenticity and confidentiality of subscriber and relying party information,
   - continuity of key and certificate lifecycle management operations, and
   - development, maintenance, and operation of CA systems integrity

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.

In our opinion, throughout the period December 1, 2016 to October 31, 2017, in all material respects:

a) Symantec disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its AATL CPS and the services and related controls provided by Verisign as enumerated in Attachment A;

b) Symantec and Verisign maintained effective controls to provide reasonable assurance that Symantec and Verisign provide its services in accordance with AATL CPS and the description of the services and related controls provided by Verisign as enumerated in Attachment A;

c) Symantec maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages is established and protected throughout their lifecycles,
   - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles,
   - subscriber information is properly authenticated (for the registration activities performed by Symantec), and
   - subordinate CA certificate requests are accurate, authenticated, and approved;

d) Symantec and Verisign, where applicable, 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.

This report does not include any representation as to the quality of Symantec's services other than its CA operations at Mountain View, California, USA and New Castle, Delaware, USA, nor the suitability of any of Symantec's services for any customer's intended purpose.

Effective at the close of business on October 31, 2017, Symantec sold its CA business operations to DigiCert Inc.

BDO USA, LLP

St. Louis, Missouri
January 31, 2018

## Attachment A

### Symantec Managed PKI Certification Practice Statement Version in Scope

| CPS Name | Version | Date |
|---|---|---|
| Symantec Managed PKI (MPKI) for Adobe@ Approved Trust List (AATL) Certification Practice Statement | 1.0 | February 9, 2015 |

### Description of Services Provided for Symantec and Related Controls Exercised by Verisign at the New Castle, Delaware Location

Symantec has entered into an agreement with Verisign Inc. (Verisign), to provide datacenter hosting services at the New Castle, Delaware datacenter (the datacenter). Verisign performs the same physical and environmental security controls as Symantec has disclosed in Section 5 and Section 6 of the Symantec Trust Network (STN) Certification Practice Statement; however, Verisign performs UPS maintenance quarterly, rather than semi-annually.

Verisign has implemented the following physical and environmental security controls to protect Symantec assets at the datacenter. Production systems housed in the datacenter are protected by multiple tiers of physical security, with access to the lower tier required before gaining access to the next highest tier. The datacenter enforces individual access control through the use of two-factor authentication, including biometrics. Physical access to the datacenter is automatically logged. Visitors to the datacenter are required to sign a log at the security office, wear a visitor badge, and be escorted while onsite. The datacenter facilities are manned continuously by on-site security personnel and the premises are continuously video monitored and recorded. Multiple generators, UPS, HVAC and fire suppression systems have been implemented at the datacenter.

## Attachment B

### List of CAs In-Scope

| **Symantec Root CAs** |
|---|
| 1. Symantec Document Signing RSA Root CA<br>2. Symantec Document Signing ECC Root CA<br>3. Symantec Test Drive Document Signing ECC Root CA<br>4. Symantec Test Drive Document Signing RSA Root CA<br>5. Symantec Class 2 Public Primary Certification Authority – G4<br>6. Symantec Class 2 Public Primary Certification Authority – G6 |
| **Symantec Signing CAs** |
| 7. Lloyd's Register Group Individual Document Signing RSA CA<br>8. Symantec Class 2 Individual Signing ECC CA<br>9. Symantec Class 2 Individual Signing RSA CA<br>10. Symantec Class 2 Signing ECC Intermediate CA<br>11. Symantec Class 2 Signing RSA Intermediate CA<br>12. Symantec Class 3 Organizational Signing ECC CA<br>13. Symantec Class 3 Organizational Signing RSA CA<br>14. Symantec Individual Document Signing ECC CA<br>15. Symantec Individual Document Signing RSA CA<br>16. Symantec Test Drive Individual Document Signing RSA CA<br>17. Symantec Test Drive Organizational Signing ECC CA |