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 the Symantec Corporation (Symantec) Certification Authority (CA) operations at Mountain View, California, USA and New Castle, Delaware 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 in:
   - Symantec Trust Network (STN) Certificate Policy (CP) versions as set out in Attachment A (including sections 1 through 9),
   - Symantec's disclosure of the services and related controls provided by Verisign in Attachment A,
   - Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement (Symantec Non-Federal SSP CPS) versions as set out in Attachment A that is consistent with the STN CP (including sections 1 through 9), and
   - Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and Symantec (including all sections);

b) the effectiveness of Symantec's controls and Verisign's controls, where applicable, over the provision of services in accordance with Symantec's disclosed practices, including the:
   - STN CP versions as set out in Attachment A (including sections 1 through 9),
   - Disclosure of the services and related controls provided by Verisign in Attachment A,
   - Symantec Non-Federal SSP CPS versions as set out in Attachment A that is consistent with the STN CP (including sections 1 through 9), and
   - Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and Symantec (including all sections);

c) the effectiveness of Symantec's controls and Verisign's controls, where applicable, over the:
   - establishment and protection of the integrity of keys and certificates it manages throughout their lifecycle,
   - establishment and protection of the integrity of subscriber keys and certificates it manages throughout their lifecycle,
   - provision for the proper authentication of subscriber information (for the registration activities performed by Symantec), and
   - establishment of accurate, authentic and approved subordinate CA requests; and

d) the effectiveness of Symantec's controls and Verisign's controls, where applicable, over the
   - restriction of logical and physical access to CA systems and data to authorized individuals,

- 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 (collectively referred to as the Non-Federal SSP CAs) as enumerated in Attachment B.

Symantec's management are 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 for the Symantec Non-Federal SSP – Customer Specific CAs as disclosed in the Symantec Non-Federal SSP CPS versions enumerated in Attachment B. Our examination did not extend to the controls exercised by these external registration authorities.

Symantec does not escrow its CA keys, does not provide certificate renewal services, and does not provide certificate 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 CAs as enumerated in Attachment B, in all material respects:

a) Symantec disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
   - STN CP versions as set out in Attachment A (including sections 1 through 9),
   - Disclosure of the services and related controls provided by Verisign in Attachment A,
   - Symantec Non-Federal SSP CPS versions as set out in Attachment A that is consistent with the STN CP (including sections 1 through 9), and
   - Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and Symantec (including all sections);

b) Symantec and Verisign, where applicable, maintained effective controls over the over the provision of services in accordance with its disclosed practices, including the:
   - STN CP versions as set out in Attachment A (including sections 1 through 9),
   - Disclosure of the services and related controls provided by Verisign in Attachment A,
   - Symantec Non-Federal SSP CPS versions as set out in Attachment A that is consistent with the STN CP (including sections 1 through 9), and
   - Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and Symantec (including all sections);

c) Symantec and Verisign, where applicable, maintained effective controls to provide reasonable assurance that:

- the integrity of keys and certificates it manages is established 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; and

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.

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 practicesin its:
- STN CP versions as set out in Attachment A (including sections 1 through 9),
- Disclosure of the services and related controls provided by Verisign in Attachment A,
- Symantec Non-Federal SSP CPS versions as set out in Attachment A that is consistent with the STN CP (including sections 1 through 9), and
- Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and Symantec (including all sections);

b) Symantec and Verisign, where applicable, maintained effective controls to provide reasonable assurance that Symantec and Verisign provide its services in accordance with Symantec's disclosed practices, including the:
- STN CP versions as set out in Attachment A (including sections 1 through 9),
- Symantec's disclosure of the services and related controls provided by Verisign in Attachment A,
- Symantec Non-Federal SSP CPS versions as set out in Attachment A that is consistent with the STN CP (including sections 1 through 9), and
- Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and Symantec (including all sections);

c) Symantec and Verisign, where applicable, 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; and

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 Certification Practice Statement and Certificate Policy Versions in Scope

Policy Name	Version	Date
Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement	2.0	September 15, 2017
Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement	1.24	April 29, 2013
Symantec Trust Network (STN) Certificate Policy	2.8.24	September 8, 2017
Symantec Trust Network (STN) Certificate Policy	2.8.23	December 19, 2016
Symantec Trust Network (STN) Certificate Policy	2.8.22	September 9, 2016
Memorandum of Agreement between the Federal PKI Policy Authority and Symantec		December 19, 2016
Memorandum of Agreement between the Federal PKI Policy Authority and Symantec		June 15, 2016

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 Intermediate CAs
1. Symantec Class 1 SSP CA - G2
2. Symantec Class 2 SSP CA - G2
3. Symantec Class 3 SSP Intermediate CA - G3
4. Symantec Non Federal SSP Organization Signing CA
5. VeriSign Class 2 SSP Intermediate CA
6. VeriSign Class 3 SSP Intermediate CA - G2
Non-federal SSP Customer Symantec Class 1 SSP CA – G2
7. NRC Rudimentary CA G2
Non-federal SSP Customer Symantec Class 2 SSP CA – G2
8. NRC Basic CA G2
Non-federal SSP Customer CAs Under Symantec Class 3 SSP Intermediate CA -G3
9. Booz Allen Hamilton Device CA 02
10. CSC CA - 2
11. CSRA FBCA C3 CA
12. CSRA FBCA C3 Device CA
13. CSRA FBCA C4 CA
14. CSRA FBCA C4 Device CA
15. Eid Passport LRA 2 CA
16. Eid Passport LRA CA 3
17. Eid Passport Content Signer CA 3
18. RAPIDGate PIV-I Agency CA
19. RAPIDGate PIV-I Device CA
20. RAPIDGate-Premier CA
21. RAPIDGate-Premier Device CA
22. Senate PIV-I CA G4
23. Senate PIV-I Device CA G2
24. Senate PIV-I Device CA G4
25. SureID Inc. CA1
26. SureID Inc. CA2
27. SureID Inc. Device CA1
28. SureID Inc. Device CA2
29. Symantec Healthcare CA

Non-federal SSP Customer CAs Under Verisign Class 2 SSP Intermediate CA
30. Fairfax County Government Basic CA
Non-federal SSP Customer CAs Under Verisign Class 3 SSP Intermediate CA -G2
31. ADP MEAS Medium HW CA
32. BAH Device CA
33. Booz Allen Hamilton CA 02
34. Booz Allen Hamilton Device CA
35. Booz Allen Hamilton Device CA 02
36. California Prison Health Care Services SSP Med HW CA
37. CSC CA-2
38. CSC Device CA-2
39. Eid Passport LRA CA 1
40. Eid Passport LRA Content Signer CA 1
41. Eid PIV-1 Test CA
42. Eid PIV-1 Test Device CA
43. HIDSigningCA2
44. HIDSigningDeviceCA1
45. ICFI Device CA
46. ICFI PIV Interoperable CA
47. JASI Device CA
48. Millennium Challenge Corporation Medium HW CA
49. Millennium Challenge Corporation Medium HW CA-G2
50. Noblis CA - G2
51. Oregon Health Authority Medium Assurance CA
52. RAPIDGate PIV-I Agency CA
53. RAPIDGate PIV-I Device CA
54. RAPIDGate-Premier CA
55. RAPIDGate-Premier Device CA
56. Senate PIV-I CA
57. Senate PIV-I CA Device G2
58. Senate PIV-I CA G2
59. Senate PIV-I Device CA
60. State of CO Device CA
61. State of Colorado Device CA G2
62. State of Colorado Medium HW CA G2
63. State of Florida AHCA Medium Assurance CA
64. State of Kansas Non Federal SSP CA G2
65. Symantec Healthcare CA
66. Symantec Non Federal SSP Organization Signing CA
67. VeriSign Class 3 SSP Intermediate CA