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 (Symantec) Certification Authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan 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 extended validation SSL (EV SSL) certificate lifecycle management business practices in its Symantec Trust Network (STN) Certification Practices Statement (CPS), the STN Certificate Policy (CP), and its disclosure of the services and related controls provided by Verisign as enumerated in Attachment A, including Symantec's commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the Symantec website;

b) the provision of such services in accordance its disclosed practices; and

c) the effectiveness of Symantec's controls and Verisign's controls, where applicable, over
   - key and EV SSL certificate integrity,
   - the authenticity and confidentiality of EV SSL subscriber and relying party information, and
   - continuity of key and EV SSL certificate lifecycle management operations

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 – Extended Validation SSL v1.6. Our responsibility is to express an opinion based on our examination.

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.

Our examination was conducted in accordance with standards for attestation engagements 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 EV SSL certificate lifecycle management business practices in its STN CPS, STN CP, and the services and related controls provided by Verisign as enumerated in Attachment A, including Symantec's commitment to provide EV SSL;

b) certificates in conformity with the CA/Browser Forum Guidelines on the Symantec website, and provided such services in accordance with its disclosed practices; and

c) Symantec and Verisign, where applicable, maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles, and
   - EV SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.

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 December 1, 2016 to October 31, 2017, in all material respects:

a) Symantec disclosed its EV SSL certificate lifecycle management business practices in its STN CPS, STN CP, and the services and related controls provided by Verisign as enumerated in Attachment A, including Symantec's commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the Symantec website, and provided such services in accordance with its disclosed practices; and

b) Symantec and Verisign, where applicable, maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles, and
   - EV SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.

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; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan nor the suitability of any of Symantec's services for any customer's intended purpose.

During the period, Symantec's internal monitoring processes and various third parties identified issues of noncompliance with respect to the CA/Browser Forum Guidelines for The Issuance And Management Of Extended Validation Certificates version 1.6.6. The software error caused 387 extended validation certificates to be issued with incorrect location information. The certificates were subsequently revoked. This issue was posted publicly in the online forums of the CA/Browser

Forum as well as the individual Internet browsers (Mozilla Bug 1413761 reported November 1, 2017). Symantec's remediation procedures have also been publicly communicated through these forums. This issue was an isolated software development error and did not have a systemic impact on the operating effectiveness of Symantec's controls. Our opinion is not modified with respect to this matter.

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

Symantec's use of the WebTrust for Certification Authorities – Extended Validation SSL 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.

BDO USA, LLP

St. Louis, Missouri
January 31, 2018

Attachment A

Symantec Trust Network Certification Practice Statement and Certificate Policy Versions in Scope

Policy Name	Version	Date
Symantec Trust Network (STN) Certification Practice Statement	3.8.28	September 8, 2017
Symantec Trust Network (STN) Certification Practice Statement	3.8.27	December 19, 2016
Symantec Trust Network (STN) Certification Practice Statement	3.8.26	September 9, 2016
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

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

Root CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Public Primary Certification Authority - G4	4C79B59A289C763164F58944D09102DE	58:D5:2D:B9:33:01:A4:FD:29:1A:8C:96:45:A0:8F:EE:7F:52:92:82	53:DF:DF:A4:E2:97:FC:FE:07:59:4E:8C:62:D5:B8:AB:06:B3:2C:75:49:F3:8A:16:30:94:FD:64:29:D5:DA:43
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Public Primary Certification Authority - G6	65637185D36F45C68F7F31F909879282	26:A1:6C:23:5A:24:72:22:9B:23:62:80:25:BC:80:97:C8:85:24:A1	B3:23:96:74:64:53:44:2F:35:3E:61:62:92:BB:20:BB:AA:5D:23:B5:46:45:0F:DB:9C:54:B8:38:61:67:D5:29
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	18DAD19E267DE8BB4A2158CDCC6B3B4A	4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5	9A:CF:AB:7E:43:C8:D8:80:D0:6B:26:2A:94:DE:EE:E4:B4:65:99:89:C3:D0:CA:F1:9B:AF:64:05:E4:1A:B7:DF
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2007 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G4	2F80FE238C0E220F486712289187ACB3	22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A	69:DD:D7:EA:90:BB:57:C9:3E:13:5D:C8:5E:A6:FC:D5:48:0B:60:32:39:BD:C4:54:FC:75:8B:2A:26:CF:7F:79
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	401AC46421B31321030EBBE4121AC51D	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54	23:99:56:11:27:A5:71:25:DE:8C:EF:EA:61:0D:DF:2F:A0:78:B5:C8:06:7F:4E:82:82:90:BF:B8:60:E8:4B:3C

Class 3 CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
C=NZ, O=IBM New Zealand Limited, OU=Symantec Trust Network, CN=IBM New Zealand Limited Public CA	7C8E8FF07BCA9C7A1AB3E26BE3729410	DC:4B:C2:BD:A3:A8:7D:5F:8F:B1:8D:73:CA:BF:BC:4E:F6:96:D6:12	A6:AE:79:59:A1:95:74:9C:A8:87:38:6F:A0:44:82:BD:16:9D:C1:15:7E:31:2D:30:1B:0D:5C:33:3F:AF:2B:02
C=US, O=Blue Coat Systems, Inc., OU=Symantec Trust Network, CN=Blue Coat Public Services Intermediate CA	51630EBDFE2D8FFC797103763D7552C3	8E:DC:EE:98:F5:78:8D:38:B8:D8:AD:0E:0C:61:37:A6:FB:D1:66:6D	AF:70:11:C3:EF:70:A7:96:26:B1:43:A7:14:99:96:FF:15:2F:75:62:85:1D:08:C3:AA:DC:DE:E8:29:9E:57:2B
C=US, O=Oracle Corporation, OU=Symantec Trust Network, CN=Oracle SSL CA - G2	3135BB7E6DE2663AB0E233E6B0E1A5CC	03:86:D9:39:CF:7B:A7:88:55:27:34:18:5B:EA:D0:B1:3E:87:39:14	E4:AF:2F:AE:41:18:7D:58:F2:09:B0:1B:1D:87:53:C2:DC:CB:3F:60:1C:E8:62:73:E3:7E:87:38:C2:A5:CC:B5
C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 3 MPKI Secure Server CA, CN=Oracle SSL CA	2585C838A4C935E383866B6BA2422FC7	4B:E8:0A:AC:65:90:EE:FE:50:08:A5:A1:DD:33:40:66:54:BA:32:2A	7F:68:89:FF:E8:B0:20:45:E2:CA:C9:9A:2F:2E:E4:F4:C2:EE:D2:49:34:B6:52:18:72:D3:4B:F8:12:67:1C:4B

Class 3 CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit EV CA - G2	71223CA522185EAC44CF1770D1A8AA5D	0B:69:D3:71:3F:1B:05:84:F1:C8:89:45:A8:5B:4C:EB:5F:CF:D7:21	66:36:36:C0:3F:D0:B5:B1:71:F2:B0:44:07:C3:DF:76:7B:34:9C:8A:99:0D:87:CE:48:58:98:16:6E:2B:51:20
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit EV CA - G3	4934B1B39646024939700C645B4F1FA0	5C:EB:F0:3C:1A:8F:E1:EA:16:19:57:AC:F9:44:66:D1:A8:8D:74:C4	4B:2C:BA:18:EF:BC:E6:C3:C4:A8:0A:AA:BC:95:23:37:00:0C:D9:34:6B:76:8D:06:24:12:A2:DE:D8:46:ED:C9
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit Extended Validation CA	4D955D20AF85C49F6925FBAB7C665F89	CA:C5:5F:77:BC:17:B2:47:B0:B9:F5:91:F5:8E:6A:E9:7B:FB:9E:1B	5A:D4:18:3B:54:F0:E2:76:2D:A8:D9:10:E1:E7:E9:F2:AB:2F:1B:C4:CE:6A:63:8F:0D:BB:F3:37:EB:4A:13:9F
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 384 bit Extended Validation CA	7A760B273C322398D3D4F86B6EBB2D50	38:CC:3D:7E:F8:69:60:4D:B3:9D:34:FD:B7:BD:66:D0:74:42:E9:B6	77:FE:87:6A:1C:47:63:49:F5:EB:9A:E9:BF:53:F7:81:4A:0A:E4:11:56:26:67:C5:8B:7E:D2:78:69:C5:40:91
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G2	366585077A8867AB58F4A094F8103733	E4:99:59:A4:B3:36:AC:BD:2D:AC:75:9B:B5:21:B9:46:03:3E:82:3A	6C:66:B7:6E:68:D6:C7:9F:AF:E5:C9:4E:9B:7D:0C:F7:53:C7:15:CC:85:38:7E:11:32:3B:79:35:F8:61:C1:87
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3	7EE14A6F6FEFF2D37F3FAD654D3ADAB4	E3:FC:0A:D8:4F:2F:5A:83:ED:6F:86:F5:67:F8:B1:4B:40:DC:BF:12	9E:6B:C5:F9:EC:C5:24:60:E8:ED:C0:2C:64:4D:1B:E1:CB:9F:23:16:F4:1D:AF:3B:61:6A:0B:20:58:29:4B:31
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G4	5398D1998C7CBF2310C0F999A0051833	A5:65:3F:4A:81:6E:00:09:7C:CF:0F:CC:65:6A:89:1B:29:BE:19:93	31:86:22:33:62:0E:78:93:30:CC:89:3E:8B:5E:66:70:53:31:B8:B8:8B:0E:D3:0A:44:57:4D:9E:0A:71:C4:F1
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL SGC CA - G2	7A0F41DF1CCD14DCB269298EE22C6A35	37:8F:E7:3E:16:E4:F1:E3:39:49:B7:60:A3:BD:22:51:49:35:90:25	B2:74:5D:0A:9B:71:D9:48:F3:4E:92:1A:F5:9F:34:2A:DF:6E:40:7D:88:BC:51:D3:8A:C5:2B:58:3A:0E:BD:15
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Extended Validation SHA256 SSL CA	09B749FD7F0B4916CA055656CFF6D982	CD:F4:28:A8:90:D3:74:8C:5D:28:ED:1F:4C:69:49:9A:3E:16:F1:33	1F:9B:31:F8:20:92:9E:BF:A0:31:17:EC:2B:77:BA:6B:0F:B6:EC:C9:E0:27:68:2A:55:93:78:DA:31:1C:54:EF
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)07, CN=VeriSign Class 3 Extended Validation 1024-bit SSL SGC CA	6EE44E2FF9761AE5C84AFFBF2552E474	FA:3E:E1:06:C9:17:CD:FF:9F:CF:46:F3:F2:25:85:FE:B7:4D:C4:CD	49:A0:3A:1A:88:D2:A7:32:E1:D6:29:FB:10:07:81:21:DE:EF:F3:33:D6:A9:8B:59:15:D3:52:13:51:2E:16:83

Class 3 CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Extended Validation CA - T1	33F5AE11193083147E5B66F31FED1129	09:BA:2F:C6:04:B7:D6:63:24:24:70:83:A4:B8:44:57:9A:B7:F0:7E	D8:05:64:43:3E:D3:5C:85:0E:2A:D5:89:B7:71:3A:4D:AC:01:A0:92:92:86:9B:DB:B8:0E:42:E2:3F:93:36:EA
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Extended Validation SGC CA - T1	1A4CE18725E5C114B8C98DE0EBA99AD6	C3:70:A4:69:A4:D2:20:BE:C8:5C:89:73:BF:C3:E6:BC:3E:09:46:B5	6E:DA:D2:26:1A:A3:D5:3B:E0:D6:FF:5F:A7:1C:34:A3:4B:25:3B:0C:63:7B:35:BF:3E:96:65:40:F7:8B:63:1B
C=US, O=Wells Fargo, OU=Symantec Trust Network, CN=Wells Fargo Certificate Authority WS1	50776F58B196C391691EE658A90A9D6B	E8:03:9D:FE:57:13:1F:11:D9:D6:77:F7:CF:7C:F5:B6:E8:9D:98:5D	C2:10:87:41:6B:BF:98:3B:9F:FE:40:F5:D5:6E:E0:FF:D9:4E:B1:E6:66:B0:4A:53:2A:DE:48:2E:C2:01:D6:7C