



## REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Symantec Corporation:

We have examined for the Thawte Certification Authority (CA) operations provided by Symantec Corporation (Symantec) at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; and Dublin, Ireland and for Verisign, Inc. (Verisign), an independent service organization that provides datacenter hosting services to Symantec for the Thawte Certification Authority operations 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 Thawte Certification Practices Statement 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 terminated the contracts for each of its three external registration authorities used for specific subscriber registration activities as disclosed in Symantec's business practices. Upon terminating these relationships, Symantec reperformed the validation work originally performed by these external registration authorities for each certificate that was still valid. The dates for termination for CrossCert, CertSuperior, and Certisur were January 19, 2017, April 4, 2017, and April 14, 2017, respectively. Our examination did not extend to the controls exercised by these external registration authorities.



Symantec does not escrow its CA keys, does not provide Integrated Circuit Card Lifecycle Management services to subscribers, 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 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 Symantec's thawte Certification Practices Statement 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 thawte Certification Practices Statement 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 the thawte Certification Practices Statements 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; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; and Dublin, Ireland, 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.

Symantec's use of the WebTrust for Certification Authorities 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

### Thawte Certification Practice Statement Versions in Scope

Policy Name	Version	Date
<a href="#">thawte Certification Practice Statement</a>	3.7.18	September 8, 2017
thawte Certification Practice Statement	3.7.17	December 19, 2016
thawte Certification Practice Statement	3.7.16	September 9, 2016

### Description of Services Provided for Symantec and Related Controls Exercised by Verisign at 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 thawte 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=thawte, Inc., OU=(c) 2007 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G2	35FC265CD9844FC93D263D579BAED756	AA:DB:BC:22:23:8F:C4:01:A1:27:BB:38:DD:F4:1D:DB:08:9E:F0:12	A4:31:0D:50:AF:18:A6:44:71:90:37:2A:86:AF:AF:8B:95:1F:FB:43:1D:83:7F:1E:56:88:B4:59:71:ED:15:57
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	344ED55720D5EDEC49F42FCE37DB2B6D	91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81	8D:72:2F:81:A9:C1:13:C0:79:1D:F1:36:A2:96:6D:B2:6C:95:0A:97:1D:B4:6B:41:99:F4:EA:54:B7:8B:FB:9F
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2008 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G3	600197B746A7EAB4B49AD64B2FF790FB	F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2	4B:03:F4:58:07:AD:70:F2:1B:FC:2C:AE:71:C9:FD:E4:60:4C:06:4C:F5:FF:B6:86:BA:E5:DB:AA:D7:FD:D3:4C
C=ZA, ST=Western Cape, L=Durbanville, O=Thawte, OU=Thawte Certification, CN=Thawte Timestamping CA	0	BE:36:A4:56:2F:B2:EE:05:DB:B3:D3:23:23:AD:F4:45:08:4E:D6:56	6B:6C:1E:01:F5:90:F5:AF:C5:FC:F8:5C:D0:B9:39:68:84:04:86:59:FC:2C:6D:11:70:D6:8B:04:52:16:C3:FD



Class 3 CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
C=US, O=Symantec Corporation, CN=Symantec Time Stamping Services CA - G2	7E93EBFB7CC64E59EA4B9A77D406FC3B	6C:07:45:3F:FD:DA:08:B8:37:07:C0:9B:82:FB:3D:15:F3:53:36:B1	06:25:FE:E1:A8:0D:7B:89:7A:97:12:24:9C:2F:55:FF:39:1D:66:61:DB:D8:B8:7F:9B:E6:F2:52:D8:8C:ED:95
C=US, O=Thawte, Inc., CN=Thawte Code Signing CA - G2	47974D7873A5BCAB0D2FB370192FCE5E	80:8D:62:64:2B:7D:1C:4A:9A:83:FD:66:7F:7A:2A:9D:24:3F:B1:C7	AF:84:0C:A2:B9:DF:B7:76:BF:81:AA:94:C4:01:BC:44:0C:52:E5:C5:90:C4:36:07:A1:3D:66:80:D8:3E:33:49
C=US, O=thawte, Inc., CN=thawte ECC EV SSL CA	1FF2FCBC6326AABD286693991F43EC21	E9:2B:D8:99:36:8C:0F:41:67:82:A5:BE:8D:F2:B9:75:66:A8:3F:6B	EA:D6:2F:42:BB:36:9D:D4:3C:F6:13:1A:C2:D8:D7:2E:4F:9F:EE:85:E6:9D:45:DA:AF:FE:32:6A:AC:2A:46:F1
C=US, O=thawte, Inc., CN=thawte EV Code Signing CA	779A2BE6DEEDA2BFB902CA8E3668B9AF	B1:7E:FE:36:89:24:DF:F5:0A:91:9C:58:A6:A8:6E:F1:81:FA:C5:6E	F3:76:F6:E5:BF:66:0F:6B:ED:B7:68:DC:D1:30:3E:AD:D4:A9:6F:2E:D7:A9:77:17:E8:78:FA:E6:BB:59:59:FA
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G2	05237150E67BDD38F33EF53CD211313F	19:73:F3:07:35:9B:C9:61:03:03:57:90:BF:75:DD:91:51:E8:3F:99	37:F6:BD:9B:EE:0C:74:F6:08:DD:47:4B:56:A7:2F:81:83:07:7D:FC:26:62:AF:79:BF:E3:D4:FA:BC:F0:B1:C4
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G3	5D72FB337620F64C7280DBE91281FF6A	68:06:0C:A0:74:FF:36:C7:E8:1B:0B:33:8D:7E:83:76:79:0E:D0:20	1A:99:01:9F:9D:41:2A:64:45:47:49:ED:AA:8E:7D:C4:66:73:D6:44:DF:3C:E1:5C:C6:55:73:5E:A0:DF:86:FE
C=US, O=thawte, Inc., CN=thawte Extended Validation SHA256 SSL CA	0A489E88537E8AA6454D6E2C4B2AEB20	14:B4:AC:F9:44:34:F7:D0:76:8D:3E:E4:8D:18:8E:FD:0C:29:13:7A	79:20:B8:E1:8D:2F:C1:2D:81:C2:FA:B9:0A:63:B1:B5:2A:B3:29:CE:7C:D1:CB:7C:A0:94:CD:F9:D6:00:F4:92
C=US, O=thawte, Inc., CN=thawte SHA256 Code Signing CA	71A0B73695DDB1AFC23B2B9A18EE54CB	D0:0C:FD:BF:46:C9:8A:83:8B:C1:0D:C4:E0:97:AE:01:52:C4:61:BC	C4:D1:8E:0A:58:E4:EF:FD:17:ED:77:C8:40:B6:13:EF:15:F5:51:07:6E:A9:2C:2B:77:F6:60:9A:6C:25:57:C7
C=US, O=thawte, Inc., CN=thawte SHA256 Code Signing CA - G2	0BF3CC63CF04304D47C3B587049FA807	F3:75:9A:4E:54:48:BA:CD:B7:85:62:32:84:61:04:58:44:21:6E:B7	F7:6F:0D:8A:D3:30:AC:FD:4C:5B:D0:5A:58:A1:CF:15:5D:E0:0B:E2:C9:8F:4E:78:99:BE:24:E8:0A:2A:BC:BF
C=US, O=thawte, Inc., CN=thawte SHA256 SSL CA	36349E18C99C2669B6562E6CE5AD7132	67:D1:47:D5:DA:B7:F2:8D:66:3C:A5:B7:A9:56:8F:08:74:27:B9:F7	3F:3A:F9:C9:CC:2C:75:99:EF:8F:6D:D7:CA:51:6C:FC:17:97:D7:D1:20:02:25:4F:3B:FD:0D:4D:0F:E9:DE:86
C=US, O=Thawte, Inc., CN=Thawte SSL CA	4D5F2C3408B24C20CD6D507E244DC9EC	73:E4:26:86:65:7A:EC:E3:54:FB:F6:85:71:23:61:65:8F:2F:43:57	08:55:41:4A:F5:F5:FD:7E:26:4F:8B:00:2A:39:CC:ED:67:E5:95:2E:89:B6:1B:68:0C:C8:47:BA:A3:49:44:DE
C=US, O=thawte, Inc., CN=thawte SSL CA - G2	1687D6886DE2300685233DBF11BF6597	2E:A7:1C:36:7D:17:8C:84:3F:D2:1D:B4:FD:B6:30:BA:54:A2:0D:C5	B7:A8:AF:2A:4A:43:F0:A8:6B:15:60:4D:E6:46:12:09:C9:CD:76:89:4D:8B:07:48:BC:99:D9:A7:97:01:3B:B0
C=US, O=Thawte, Inc., OU=Domain Validated SSL, CN=Thawte DV SSL CA	7610128A17B682BB3A1F9D1A9A35C092	3C:A9:58:F3:E7:D6:83:7E:1C:1A:CF:8B:0F:6A:2E:6D:48:7D:67:62	D2:57:38:31:FA:53:76:B1:C7:DC:0D:BB:0E:F5:88:13:E9:07:06:18:FA:5A:21:E1:3F:5E:9F:2B:65:E0:A3:20



Class 3 CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
C=US, O=thawte, Inc., OU=Domain Validated SSL, CN=thawte DV SSL CA - G2	2C69E12F6A670BD99D D20F919EF09E51	4C:03:68:21:E4:34:13:B6:63: B0:6D:CF:01:4C:E9:0D:50:34: 7F:99	9F:25:11:A2:3E:70:D9:5F:B6: 27:98:50:8A:67:6C:C3:89:64: 10:09:36:A6:E6:D3:CA:E7:71: 54:C0:29:0F:02
C=US, O=thawte, Inc., OU=Domain Validated SSL, CN=thawte DV SSL SHA256 CA	3E23345AED2C0A517B 26DED4801D10AA	50:F1:25:EF:CA:24:28:FF:17: D2:04:B8:9E:52:64:50:9A:28: 3D:A7	53:7C:5C:80:72:36:3E:14:7C: 84:D2:1D:0D:22:48:B6:B9:9A: 9A:8A:43:31:16:59:83:5E:C3: 39:26:DA:28:60