



Tel: 314-889-1100

Fax: 314-889-1101

[www.bdo.com](http://www.bdo.com)

101 S Hanley Rd, #800

St. Louis, MO 63105

## REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of DigiCert, Inc. (“DigiCert”):

We have examined DigiCert management’s [assertion](#) that for its Certification Authority (“CA”) operations at various locations in the United States of America, throughout the period April 1, 2019 to October 31, 2019 for its CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement and DigiCert Certificate Policy enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#). DigiCert’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

The relative effectiveness and significance of specific controls at DigiCert 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 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 management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.



Because of the nature and inherent limitations of controls, DigiCert’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 management’s assertion, as referred to above, is fairly stated, in all material respects.

Without modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter Description
1	Certificate Content and Revocation	DigiCert was notified in <a href="#">Mozilla Bug 1551363</a> of eight (8) certificates having been issued containing the phrase "Some-State" in the stateOrProvinceName field. Upon notification, DigiCert launched an internal investigation and discovered several thousand certificates that included additional errors in the locality field. These errors have been disclosed separately in <a href="#">Mozilla Bug 1576013</a> .
2	Certificate Self-audit	For the final three (3) months of the engagement period, self-assessments for at least three percent (3%) of certificates issued were not performed in a timely manner.

We have noted any instances possible non-conformance that are relevant to the CAs enumerated in [Attachment B](#). DigiCert’s assertion notes all instances possible non-conformance, addressed by DigiCert, during the engagement period, regardless of the particular CAs enumerated in [Attachment B](#).

This report does not include any representation as to the quality of DigiCert’s services other than its CA operations at various locations in the United States of America, nor the suitability of any of DigiCert’s services for any customer’s intended purpose.

DigiCert’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

January 29, 2020



**Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope**

<b>Policy Name</b>	<b>Version</b>	<b>Date</b>
<a href="#">DigiCert Certification Practices Statement</a>	4.19	July 25, 2019
DigiCert Certification Practices Statement	4.18	April 17, 2019
DigiCert Certification Practices Statement	4.17	March 1, 2019
<a href="#">DigiCert Certificate Policy</a>	4.19	July 25, 2019
DigiCert Certificate Policy	4.18	April 17, 2019
DigiCert Certificate Policy	4.17	March 1, 2019



## Attachment B - List of CAs In-Scope

Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Baltimore CyberTrust Root	16AF57A9F676B0AB126095AA5EBADEF22AB31119D644AC95CD4B93DBF3F26AEB	5/12/2000	5/12/2025
Cybertrust Global Root	802447EE521CC666CDB7BBAE93A385E55F200D76A3D1356A85445AC4CDBBED12	1/8/2014	12/15/2030
Cybertrust Global Root	960ADF0063E96356750C2965DD0A0867DA0B9CBD6E77714AEAFB2349AB393DA3	12/15/2006	12/15/2021
DigiCert Assured ID Root CA	3E9099B5015E8F486C00BCEA9D111EE721FABA355A89BCF1DF69561E3DC6325C	11/10/2006	11/10/2031
DigiCert Assured ID Root G2	7D05EBB682339F8C9451EE094EEBFefa7953A114EDB2F44949452FAB7D2FC185	8/1/2013	1/15/2038
DigiCert Assured ID Root G3	7E37CB8B4C47090CAB36551BA6F45DB840680FBA166A952DB100717F43053FC2	8/1/2013	1/15/2038
DigiCert Global Root CA	4348A0E9444C78CB265E058D5E8944B4D84F9662BD26DB257F8934A443C70161	11/10/2006	11/10/2031
DigiCert Global Root G2	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F	8/1/2013	1/15/2038
DigiCert Global Root G3	31AD6648F8104138C738F39EA4320133393E3A18CC02296EF97C2AC9EF6731D0	8/1/2013	1/15/2038
DigiCert High Assurance EV Root CA	7431E5F4C3C1CE4690774F0B61E05440883BA9A01ED00BA6ABD7806ED3B118CF	11/10/2006	11/10/2031
DigiCert Trusted Root G4	552F7BDCF1A7AF9E6CE672017F4F12ABF77240C78E761AC203D1D9D20AC89988	8/1/2013	1/15/2038
Verizon Global Root CA	68AD50909B04363C605EF13581A939FF2C96372E3F12325B0A6861E1D59F6603	7/30/2009	7/30/2034

Cross-Signed Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Cybertrust Global Root	24905145BD9B9BFE99C60354B49951BE0E709F1634CFBD0E370FEB9F068ED6C3	12/3/2014	12/3/2024
Cybertrust Global Root	64B3542D1BC972F58A1D179F3D0B9652BE434F3AE3842E0C447880D4D623A4DE	4/23/2014	4/23/2024
Cybertrust Global Root	9BB5CC8427AF276BF216A748AD25785D17ACBABBDE4282E606DA5262CD940F38	8/18/2010	8/18/2020
Cybertrust Global Root	9F61D09768DA33F7F99F7E7EAD935902224943B4C9AD07B629F745C0B08475B7	4/23/2014	4/23/2021
Cybertrust Global Root	D775784887CDBD7E9FCB2A9D589D367A0B6238DA1EAF51DC71C99B89B99229E0	4/23/2014	4/23/2021
Cybertrust Global Root	E71D8C3BAF43F6B3352DF574A9F0D4A2065BF03DA179514B1FCC5D9BEC8C8FCD	12/3/2014	12/3/2024
DigiCert Global Root CA	6DACBB8945137B1DAD4211B0436EFBE06F12ACE36904973B45AE25740823D369	12/7/2016	5/10/2025



Cross-Signed Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Global Root G2	2D4FAD3455AB61397401ABBB518922F84336B67E02FC8D2DB283825C4AB981BB	11/6/2017	11/5/2022
DigiCert Global Root G2	AADADD5A879D2EB8C41A89597291292709D42052F5B6399541C694C3B7353CD1	4/3/2018	4/2/2028
DigiCert Global Root G3	53A5E32ACC5714ED20C7778C655D1EE97EC07156074C8B016E2CFC73E9D2712B	11/6/2017	11/5/2022
DigiCert High Assurance EV Root CA	89DAADB41BA698BB378AEE84EAC96121D20F8C2FCA63EC686D9307229AD3EB2E	6/18/2014	6/18/2021
DigiCert High Assurance EV Root CA	BF0ADF6F1FD218CFA27F3884CE2AA6AF2AF5481C6878BFE3A6CA62515898B115	7/25/2012	7/25/2019
DigiCert High Assurance EV Root CA	CBF8FB77660167E6BAACD0DF77CDA397D0117EE2BEEA23B935317F8BB5B5E3B0	12/7/2016	5/10/2025
DigiCert Trusted Root G4	AD8EB32C9DA91DDC855F382745990147DC6F23D9FBB04FC9D476B1EE20FC71D8	7/1/2013	10/22/2023
Verizon Global Root CA	B90EEAE931E5E2B7D335F149DA6C2210986000D214FFDB62A72F7332D63731AF	4/9/2014	4/9/2024
Verizon Global Root CA	D96CBC03B523CD3315918651CF4862162887DD563AFB2352D3F34BB94576F93D	5/13/2014	5/13/2024

Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Baltimore EV CA	D46931E0182DD655EA0C16E6DD99F8E61AFFE401F734C6CA8EA0056A968EAF81	10/14/2015	5/10/2025
Cybertrust Japan ECC EV CA	92E3770B1EB44F84C2F2CB0097C2FD7126BD212B41C2610E78DDDFD8946761738	8/24/2017	8/24/2032
DigiCert Extended Validation CA G3	7C0912E5DE8478BB86E8EA46BA5AE65DC3870BCEFCBC2F46795EEECF648CFBE7	11/11/2015	11/11/2030
Aetna Inc. Secure EV CA	0A163600631BD66267FB7AEAD25C538B2B7D72AD6416A2BBD285F654BB642F6D	12/9/2014	12/9/2024
Aetna Inc. Secure EV CA2	1DDFDDF883E3945B2CB24FA5B83788379C5AB058422AB979DF66C77473988687	12/8/2017	12/8/2027
Cybertrust Japan Extended Validation Server CA	0E10BDDEE7512DBD79EBF0B4F48FEED7C83C2BD3DD81765565F4FF110B7BFA42	12/7/2016	12/7/2031
DigiCert ECC Extended Validation Server CA	FDC8986CFAC4F35F1ACD517E0F61B879882AE076E2BA80B77BD3F0FE5CEF8862	6/21/2016	6/21/2031
DigiCert Extended Validation Intermediate CA (SHA2)	802C2AD1D215E57CDC9010EA437ACE399B657194FBD40E3BB5E00B080E6496DF	12/7/2011	12/7/2026
DigiCert High Assurance EV CA-1	4C4943B9EAA14EA2A69B8A7E4D8DA89081EEA11C87E8229B9B74F68A7AD33B79	11/10/2006	11/10/2021
DigiCert High Assurance EV CA-1	541AF019961760EF19E8FB4134E6D43085B5E5E087F30197DC42B2097E10487E	11/9/2007	11/10/2021
DigiCert High Assurance EV CA-1	8FC1469B8005BFEBDBF67F514E795FE1F17EA239A2A6934857F2428ADCE6D24F	11/10/2007	11/10/2021
DigiCert High Assurance EV CA-2	1188F831C949A62E9CD4F60E36F72544F0AF924DE07F9DA992E26E44C996EEE0	3/23/2007	3/23/2022



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert SHA2 Extended Validation Server CA <sup>1</sup>	403E062A2653059113285BAF80A0D4AE422C848C9F78FAD01FC94BC5B87FEF1A	10/22/2013	10/22/2028
SecurityMetrics DigiCert EV CA	6B2328E7FFF598B2ADF90B7F3EA42B45FA606D78E2B117B7D60E99E828CF7565	10/30/2012	10/30/2022
WoSign EV SSL Pro CA	891EE2E23282E5076C9AE9047DE8EA900E066F81D6DCD9B843C59078B0F105BC	5/23/2017	5/23/2027
WoTrus EV SSL Pro CA	070531383CCD100D3E9CD964DB07AA5E845A0686F2EAE3BC8A627B182057B1F1	2/9/2018	2/9/2028
DC Government SHA2 EV Intermediate CA	F12241EE34C03A608D34DBC0EA465E1BD1AA13091554F9D4D086253FF3CE83D4	7/13/2017	7/13/2027
DigiCert EV Server CA G4	710024B37BD9F0E1537C18A4C20F9A31C4B485D1248C643F20B4C00F3716BA85	1/17/2017	1/17/2032
Secure Site Extended Validation CA	1A8D790AF9B2B34D7DD6AF61B5AA4CF1380B86095CBAC2BCAB35BD566D0180C3	4/27/2018	4/27/2028
Secure Site Pro Extended Validation CA	3883E6DE4917A46B594ECC2D2AC6A95D43E7EAA8E089A91F9BC104FF16DF8DE6	4/27/2018	4/27/2028
Secure Site Pro Extended Validation ECC CA	C3804DE51E8C17052220AE1CAD3D383E54D5B7DC28843C42F0DBD9913C1E8658	4/27/2018	4/27/2028
DigiCert High Assurance EV Root CA	071B8B4B13AD7B2BE09FDD7FBDF3482460838098C21519B83B3150F8E919832D	8/13/2018	11/4/2022
DigiCert Extended Validation CG CA	38FDF62507CEDEE16B1455E96BD23D5C6F6C5654D68C7E3B27238D2C73744A86	9/24/2018	12/14/2021
DigiCert Secure Site Korea EV CA	C022D5CEAA275F2A6268FA79AC35653B3A730DEFA41F9CD8817D6D159BD33097	3/25/2019	3/25/2029
DigiCert Secure Site Korea EV ECC CA	B0505BF2947F0807ABAE2D42C19343EAF08D1DDE3F8745B0589A57362792E470	3/25/2019	3/25/2029
TrustAsia ECC EV TLS Pro CA	2DAAC6FDFAC16C548C53FF1198254D7E937761D22A1E7CC5C1A9462E971461F5	4/27/2018	4/27/2028
TrustAsia EV TLS Pro CA	4AFFE4FEF39464D1788C660AF591D5E601B261C4811DF0A3DD9D61CAFE8E5ED8	4/27/2018	4/27/2028
DigiCert CN RSA EV CA G1	B131905CC7221270613B529AC9E786AA230ABFE154A0ACBE452BC350BD1EFE4B	6/20/2019	6/20/2029
DigiCert Extended Validation CA-2 G3	9DB1436C8F6A754C492938363D3AD8C6CDDF15381271EF1A8931DFDA386F7BB3	10/16/2019	10/16/2029
DigiCert SHA2 Extended Validation Server CA-2	3B34575D8EDD8647BAE22F23E8DE47AFB35E99ABD35FD38EF60B7F2B2BF9B518	10/16/2019	10/16/2029
TrustCubes ICA G1	2106CC7907C64B8A5DA2FC338EE94DFFF10EF711DEDDB4FC694EE092EC532B1D	7/18/2018	7/18/2028

<sup>1</sup> This CA was only in the scope of this engagement for the period April 1, 2019 to May 31, 2019. For the remainder of this period, this CA is covered under a different WebTrust report.



## DIGICERT, INC. MANAGEMENT’S ASSERTION

DigiCert, Inc. (“DigiCert”) operates the Certification Authority (“CA”) for its CAs as enumerated in [Attachment B](#) and provides extended validation SSL (“EV SSL”) CA services.

DigiCert management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its EV SSL CA services at various locations in the United States of America, throughout the period April 1, 2019 to October 31, 2019, DigiCert has:

- disclosed its EV SSL certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement and DigiCert Certificate Policy enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#).

DigiCert has disclosed the following matters publicly on Mozilla’s Bugzilla platform:

Mozilla Bug #	Description	Date Opened	Date Closed
<a href="#">Bugzilla 1515564</a>	DigiCert: Underscore character certificates	12/19/18	12/21/18
<a href="#">Bugzilla 1515788</a>	DigiCert: Underscores - CVS Pharmacy	12/20/18	02/11/19
<a href="#">Bugzilla 1516453</a>	DigiCert: Underscores - Discover	12/26/18	02/14/19
<a href="#">Bugzilla 1516545</a>	DigiCert: Underscores - Verizon	12/27/18	03/03/19
<a href="#">Bugzilla 1516561</a>	DigiCert: Underscores - Canadian Imperial Bank of Commerce	12/27/18	02/26/19
<a href="#">Bugzilla 1516599</a>	DigiCert: Underscores - Ericsson	12/27/18	05/01/19
<a href="#">Bugzilla 1517617</a>	DigiCert: Underscores - Citi	01/03/19	05/01/19
<a href="#">Bugzilla 1518555</a>	DigiCert: Use of forbidden subjectPublicKeyInfo algorithm	01/08/19	01/15/19
<a href="#">Bugzilla 1519572</a>	DigiCert: Underscores - Intuit	01/11/19	05/01/19
<a href="#">Bugzilla 1523676</a>	DigiCert: Good OCSP Responses for Revoked Intermediates	01/29/19	04/04/19
<a href="#">Bugzilla 1524875</a>	DigiCert: IP in dnsName	02/03/19	05/17/19
<a href="#">Bugzilla 1526154</a>	DigiCert: Missed Underscore Certificate Revocations	02/07/19	04/25/19



<b>Mozilla Bug #</b>	<b>Description</b>	<b>Date Opened</b>	<b>Date Closed</b>
<a href="#">Bugzilla 1527423</a>	DigiCert: P-384,ecdsa-with-SHA512 Certificates	02/12/19	07/18/19
<a href="#">Bugzilla 1531817</a>	DigiCert: in-addr.arpa Misissuance	03/01/19	07/01/19
<a href="#">Bugzilla 1533655</a>	DigiCert: Apple: Non-compliant Serial Numbers	03/07/19	07/20/19
<a href="#">Bugzilla 1539296</a>	DigiCert: KPN Outdated Audit	03/26/19	06/29/19
<a href="#">Bugzilla 1548716</a>	DigiCert: Verizon: "Default City" in Subject:localityName	05/02/19	05/20/19
<a href="#">Bugzilla 1548719</a>	DigiCert: Revoked intermediate certificates not in CRL	05/02/19	08/06/19
<a href="#">Bugzilla 1550645</a>	Digicert: CAA Checking Issue	05/09/19	Open as of report date
<a href="#">Bugzilla 1551363</a>	DigiCert: "Some-State" in stateOrProvinceName	05/13/19	09/06/19
<a href="#">Bugzilla 1556906</a>	DigiCert: Apple: Non-compliant Common Name Length	06/04/19	12/24/19
<a href="#">Bugzilla 1556948</a>	DigiCert Validation Scope Incident	06/04/19	11/26/19
<a href="#">Bugzilla 1563573</a>	DigiCert: Failure to disclose Unconstrained Intermediate within 7 Days	07/04/19	Open as of report date
<a href="#">Bugzilla 1566162</a>	DigiCert: Failure to supervise ABB Subordinate CA	07/15/19	09/15/19
<a href="#">Bugzilla 1573937</a>	DigiCert/Verizon: Qualified 2019 Audit Statements	08/14/19	Open as of report date
<a href="#">Bugzilla 1575125</a>	DigiCert: Apple: Unconstrained CAs not included in WTBR report	08/19/19	10/18/19
<a href="#">Bugzilla 1576013</a>	DigiCert: JOI Issue	08/22/19	Open as of report date
<a href="#">Bugzilla 1577014</a>	DigiCert OCSP services returns 1 byte	08/27/19	10/22/19
<a href="#">Bugzilla 1582519</a>	DigiCert: Apple: Precertificates without corresponding certificates return OCSP value of "unknown"	09/19/19	10/05/19
<a href="#">Bugzilla 1586604</a>	DigiCert: TERENA: No localityName in EV precert	10/06/19	10/08/19
<a href="#">Bugzilla 1593814</a>	DigiCert: & character in a printableString in ICA	11/04/19	12/24/19
<a href="#">Bugzilla 1595921</a>	DigiCert: Domain validation skipped	11/12/19	Open as of report date
<a href="#">Bugzilla 1596931</a>	DigiCert: Verizon CPS lacks problem reporting instructions	11/15/19	12/03/19





DigiCert, Inc.

A handwritten signature in black ink, appearing to read 'Dan Timpson', is displayed on a light gray rectangular background.

---

Dan Timpson  
Chief Technology Officer

January 29, 2020



**Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope**

<b>Policy Name</b>	<b>Version</b>	<b>Date</b>
<a href="#">DigiCert Certification Practices Statement</a>	4.19	July 25, 2019
DigiCert Certification Practices Statement	4.18	April 17, 2019
DigiCert Certification Practices Statement	4.17	March 1, 2019
<a href="#">DigiCert Certificate Policy</a>	4.19	July 25, 2019
DigiCert Certificate Policy	4.18	April 17, 2019
DigiCert Certificate Policy	4.17	March 1, 2019



## Attachment B - List of CAs In-Scope

Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Baltimore CyberTrust Root	16AF57A9F676B0AB126095AA5EBADEF22AB31119D644AC95CD4B93DBF3F26AEB	5/12/2000	5/12/2025
Cybertrust Global Root	802447EE521CC666CDB7BBAE93A385E55F200D76A3D1356A85445AC4CDBBED12	1/8/2014	12/15/2030
Cybertrust Global Root	960ADF0063E96356750C2965DD0A0867DA0B9CBD6E77714AEAFB2349AB393DA3	12/15/2006	12/15/2021
DigiCert Assured ID Root CA	3E9099B5015E8F486C00BCEA9D111EE721FABA355A89BCF1DF69561E3DC6325C	11/10/2006	11/10/2031
DigiCert Assured ID Root G2	7D05EBB682339F8C9451EE094EEBFEDA7953A114EDB2F44949452FAB7D2FC185	8/1/2013	1/15/2038
DigiCert Assured ID Root G3	7E37CB8B4C47090CAB36551BA6F45DB840680FBA166A952DB100717F43053FC2	8/1/2013	1/15/2038
DigiCert Global Root CA	4348A0E9444C78CB265E058D5E8944B4D84F9662BD26DB257F8934A443C70161	11/10/2006	11/10/2031
DigiCert Global Root G2	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F	8/1/2013	1/15/2038
DigiCert Global Root G3	31AD6648F8104138C738F39EA4320133393E3A18CC02296EF97C2AC9EF6731D0	8/1/2013	1/15/2038
DigiCert High Assurance EV Root CA	7431E5F4C3C1CE4690774F0B61E05440883BA9A01ED00BA6ABD7806ED3B118CF	11/10/2006	11/10/2031
DigiCert Trusted Root G4	552F7BDCF1A7AF9E6CE672017F4F12ABF77240C78E761AC203D1D9D20AC89988	8/1/2013	1/15/2038
Verizon Global Root CA	68AD50909B04363C605EF13581A939FF2C96372E3F12325B0A6861E1D59F6603	7/30/2009	7/30/2034

Cross-Signed Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Cybertrust Global Root	24905145BD9B9BFE99C60354B49951BE0E709F1634CFBD0E370FEB9F068ED6C3	12/3/2014	12/3/2024
Cybertrust Global Root	64B3542D1BC972F58A1D179F3D0B9652BE434F3AE3842E0C447880D4D623A4DE	4/23/2014	4/23/2024
Cybertrust Global Root	9BB5CC8427AF276BF216A748AD25785D17ACBABDDE4282E606DA5262CD940F38	8/18/2010	8/18/2020
Cybertrust Global Root	9F61D09768DA33F7F99F7E7EAD935902224943B4C9AD07B629F745C0B08475B7	4/23/2014	4/23/2021
Cybertrust Global Root	D775784887CDBD7E9FCB2A9D589D367A0B6238DA1EAF51DC71C99B89B99229E0	4/23/2014	4/23/2021
Cybertrust Global Root	E71D8C3BAF43F6B3352DF574A9F0D4A2065BF03DA179514B1FCC5D9BEC8C8FCD	12/3/2014	12/3/2024
DigiCert Global Root CA	6DACBB8945137B1DAD4211B0436EFBE06F12ACE36904973B45AE25740823D369	12/7/2016	5/10/2025



Cross-Signed Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Global Root G2	2D4FAD3455AB61397401ABBB518922F84336B67E02FC8D2DB283825C4AB981BB	11/6/2017	11/5/2022
DigiCert Global Root G2	AADADD5A879D2EB8C41A89597291292709D42052F5B6399541C694C3B7353CD1	4/3/2018	4/2/2028
DigiCert Global Root G3	53A5E32ACC5714ED20C7778C655D1EE97EC07156074C8B016E2CFC73E9D2712B	11/6/2017	11/5/2022
DigiCert High Assurance EV Root CA	89DAADB41BA698BB378AEE84EAC96121D20F8C2FCA63EC686D9307229AD3EB2E	6/18/2014	6/18/2021
DigiCert High Assurance EV Root CA	BF0ADF6F1FD218CFA27F3884CE2AA6AF2AF5481C6878BFE3A6CA62515898B115	7/25/2012	7/25/2019
DigiCert High Assurance EV Root CA	CBF8FB77660167E6BAACD0DF77CDA397D0117EE2BEEA23B935317F8BB5B5E3B0	12/7/2016	5/10/2025
DigiCert Trusted Root G4	AD8EB32C9DA91DDC855F382745990147DC6F23D9FBB04FC9D476B1EE20FC71D8	7/1/2013	10/22/2023
Verizon Global Root CA	B90EEAE931E5E2B7D335F149DA6C2210986000D214FFDB62A72F7332D63731AF	4/9/2014	4/9/2024
Verizon Global Root CA	D96CBC03B523CD3315918651CF4862162887DD563AFB2352D3F34BB94576F93D	5/13/2014	5/13/2024

Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Baltimore EV CA	D46931E0182DD655EA0C16E6DD99F8E61AFFE401F734C6CA8EA0056A968EAF81	10/14/2015	5/10/2025
Cybertrust Japan ECC EV CA	92E3770B1EB44F84C2F2CB0097C2FD7126BD212B41C2610E78DDFD8946761738	8/24/2017	8/24/2032
DigiCert Extended Validation CA G3	7C0912E5DE8478BB86E8EA46BA5AE65DC3870BCEFCBC2F46795EEECF648CFBE7	11/11/2015	11/11/2030
Aetna Inc. Secure EV CA	0A163600631BD66267FB7AEAD25C538B2B7D72AD6416A2BBD285F654BB642F6D	12/9/2014	12/9/2024
Aetna Inc. Secure EV CA2	1DDFDDF883E3945B2CB24FA5B83788379C5AB058422AB979DF66C77473988687	12/8/2017	12/8/2027
Cybertrust Japan Extended Validation Server CA	0E10BDDEE7512DBD79EBF0B4F48FEED7C83C2BD3DD81765565F4FF110B7BFA42	12/7/2016	12/7/2031
DigiCert ECC Extended Validation Server CA	FDC8986CFAC4F35F1ACD517E0F61B879882AE076E2BA80B77BD3F0FE5CECF8862	6/21/2016	6/21/2031
DigiCert Extended Validation Intermediate CA (SHA2)	802C2AD1D215E57CDC9010EA437ACE399B657194FBD40E3BB5E00B080E6496DF	12/7/2011	12/7/2026
DigiCert High Assurance EV CA-1	4C4943B9EAA14EA2A69B8A7E4D8DA89081EEA11C87E8229B9B74F68A7AD33B79	11/10/2006	11/10/2021
DigiCert High Assurance EV CA-1	541AF019961760EF19E8FB4134E6D43085B5E5E087F30197DC42B2097E10487E	11/9/2007	11/10/2021
DigiCert High Assurance EV CA-1	8FC1469B8005BFEBDBF67F514E795FE1F17EA239A2A6934857F2428ADCE6D24F	11/10/2007	11/10/2021



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert High Assurance EV CA-2	1188F831C949A62E9CD4F60E36F72544F0AF924DE07F9DA992E26E44C996EEEE0	3/23/2007	3/23/2022
DigiCert SHA2 Extended Validation Server CA <sup>1</sup>	403E062A2653059113285BAF80A0D4AE422C848C9F78FAD01FC94BC5B87FEF1A	10/22/2013	10/22/2028
SecurityMetrics DigiCert EV CA	6B2328E7FFF598B2ADF90B7F3EA42B45FA606D78E2B117B7D60E99E828CF7565	10/30/2012	10/30/2022
WoSign EV SSL Pro CA	891EE2E23282E5076C9AE9047DE8EA900E066F81D6DCD9B843C59078B0F105BC	5/23/2017	5/23/2027
WoTrus EV SSL Pro CA	070531383CCD100D3E9CD964DB07AA5E845A0686F2EAE3BC8A627B182057B1F1	2/9/2018	2/9/2028
DC Government SHA2 EV Intermediate CA	F12241EE34C03A608D34DBC0EA465E1BD1AA13091554F9D4D086253FF3CE83D4	7/13/2017	7/13/2027
DigiCert EV Server CA G4	710024B37BD9F0E1537C18A4C20F9A31C4B485D1248C643F20B4C00F3716BA85	1/17/2017	1/17/2032
Secure Site Extended Validation CA	1A8D790AF9B2B34D7DD6AF61B5AA4CF1380B86095CBAC2BCAB35BD566D0180C3	4/27/2018	4/27/2028
Secure Site Pro Extended Validation CA	3883E6DE4917A46B594ECC2D2AC6A95D43E7EAA8E089A91F9BC104FF16DF8DE6	4/27/2018	4/27/2028
Secure Site Pro Extended Validation ECC CA	C3804DE51E8C17052220AE1CAD3D383E54D5B7DC28843C42F0DBD9913C1E8658	4/27/2018	4/27/2028
DigiCert High Assurance EV Root CA	071B8B4B13AD7B2BE09FDD7FBDF3482460838098C21519B83B3150F8E919832D	8/13/2018	11/4/2022
DigiCert Extended Validation CG CA	38FDF62507CEDEE16B1455E96BD23D5C6F6C5654D68C7E3B27238D2C73744A86	9/24/2018	12/14/2021
DigiCert Secure Site Korea EV CA	C022D5CEAA275F2A6268FA79AC35653B3A730DEFA41F9CD8817D6D159BD33097	3/25/2019	3/25/2029
DigiCert Secure Site Korea EV ECC CA	B0505BF2947F0807ABAE2D42C19343EAF08D1DDE3F8745B0589A57362792E470	3/25/2019	3/25/2029
TrustAsia ECC EV TLS Pro CA	2DAAC6FDFAC16C548C53FF1198254D7E937761D22A1E7CC5C1A9462E971461F5	4/27/2018	4/27/2028
TrustAsia EV TLS Pro CA	4AFFE4FEF39464D1788C660AF591D5E601B261C4811DF0A3DD9D61CAFE8E5ED8	4/27/2018	4/27/2028
DigiCert CN RSA EV CA G1	B131905CC7221270613B529AC9E786AA230ABFE154A0ACBE452BC350BD1EFE4B	6/20/2019	6/20/2029
DigiCert Extended Validation CA-2 G3	9DB1436C8F6A754C492938363D3AD8C6CDDF15381271EF1A8931DFDA386F7BB3	10/16/2019	10/16/2029
DigiCert SHA2 Extended Validation Server CA-2	3B34575D8EDD8647BAE22F23E8DE47AFB35E99ABD35FD38EF60B7F2B2BF9B518	10/16/2019	10/16/2029
TrustCubes ICA G1	2106CC7907C64B8A5DA2FC338EE94DFFF10EF711DEDDB4FC694EE092EC532B1D	7/18/2018	7/18/2028

<sup>1</sup> This CA was only in the scope of this assertion for the period April 1, 2019 to May 31, 2019. For the remainder of this period, this CA is covered under a different WebTrust report.



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 DigiCert, Inc. (“DigiCert”):

We have examined DigiCert management’s [assertion](#) that for its Symantec Certification Authority (“CA”) operations at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, throughout the period November 1, 2018 to October 31, 2019 for CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certificate Policy for Symantec Trust Network (STN) and DigiCert Certification Practices Statement for Symantec Trust Network (STN) enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#). DigiCert’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

The relative effectiveness and significance of specific controls at DigiCert 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 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 management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.



Because of the nature and inherent limitations of controls, DigiCert'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 management's assertion, as referred to above, is fairly stated, in all material respects.

We did not note any instances of possible non-conformance relevant to the CAs enumerated in [Attachment B](#). DigiCert's assertion notes all instances possible non-conformance, addressed by DigiCert, during the engagement period, regardless of the particular CAs enumerated in [Attachment B](#).

This report does not include any representation as to the quality of DigiCert's services other than its Symantec CA operations at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, nor the suitability of any of DigiCert's services for any customer's intended purpose.

DigiCert'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.

BDS USA, LLP

January 29, 2020



## Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
<a href="#">DigiCert Certification Practices Statement for Symantec Trust Network (STN)</a>	3.13	June 25, 2019
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.12	April 18, 2019
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.11	March 18, 2019
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.10	November 2, 2018
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.9	September 11, 2018
<a href="#">DigiCert Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018





## Attachment B - List of CAs In-Scope

Root CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
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	69DDD7EA90BB57C93E135DC85EA6FCD5480B603239BDC454FC758B2A26CF7F79	11/5/2007	1/18/2038
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Public Primary Certification Authority - G6	B32396746453442F353E616292BB20BBA5D23B546450FDB9C54B8386167D529	10/18/2012	12/1/2037
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	2399561127A57125DE8CEFEA610DDF2FA078B5C8067F4E828290BFB860E84B3C	4/2/2008	12/1/2037
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	9ACFAB7E43C8D880D06B262A94DEEEE4B4659989C3D0CAF19BAF6405E41AB7DF	11/8/2006	7/16/2036
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Public Primary Certification Authority - G4	53DFDFA4E297FCFE07594E8C62D5B8AB06B32C7549F38A163094FD6429D5DA43	10/18/2012	12/1/2037
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Web PKI ECC Root - G1	92BB72F15EB75DE467C84B438181034BDAE9A016EC26434BEE3C9BBAD8CD8AF0	9/21/2017	9/20/2042
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Web PKI RSA Root - G1	F6BB5B7985A8736594C14679FA31603814502AAEB5F4282A69985DC84A450777	9/21/2017	9/20/2042

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G2	6C66B76E68D6C79FAFE5C94E9B7D0CF753C715CC85387E11323B7935F861C187	10/31/2013	10/30/2023
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3	9E6BC5F9ECC52460E8EDC02C644D1BE1CB9F2316F41DAF3B616A0B2058294B31	10/31/2013	10/30/2023



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL SGC CA - G2	B2745D0A9B71D948F34E921AF59F342ADF6E407D88BC51D38AC52B583A0EBD15	10/31/2013	10/30/2023
C=US, O=Wells Fargo, OU=Symantec Trust Network, CN=Wells Fargo Certificate Authority WS1	C21087416BBF983B9FFE40F5D56EE0FFD94EB1E666B04A532ADE482EC201D67C	8/25/2015	8/24/2025
C=US, O=Oracle Corporation, OU=Symantec Trust Network, CN=Oracle SSL CA - G2	E4AF2FAE41187D58F209B01B1D8753C2DCCB3F601CE86273E37E8738C2A5CCB5	1/6/2015	1/5/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G4	31862233620E789330CC893E8B5E66705331B8B88B0ED30A44574D9E0A71C4F1	1/7/2016	1/6/2026
C=NZ, O=IBM New Zealand Limited, OU=Symantec Trust Network, CN=IBM New Zealand Limited Public CA	A6AE7959A195749CA887386FA04482BD169DC1157E312D301B0D5C333FAF2B02	2/3/2015	2/2/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit EV CA - G2	663636C03FD0B5B171F2B04407C3DF767B349C8A990D87CE485898166E2B5120	5/12/2015	5/11/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit Extended Validation CA	5AD4183B54F0E2762DA8D910E1E7E9F2AB2F1BC4CE6A638F0DBBF337EB4A139F	12/20/2012	12/19/2022
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit EV CA - G3	4B2CBA18EFBCE6C3C4A80AAABC952337000CD9346B768D062412A2DED846EDC9	1/7/2016	1/6/2026
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 384 bit Extended Validation CA	77FE876A1C476349F5EB9AE9BF53F7814A0AE411562667C58B7ED27869C54091	12/20/2012	12/19/2022



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at <a href="https://www.verisign.com/rpa">https://www.verisign.com/rpa</a> (c)10, CN=VeriSign Class 3 Extended Validation CA - T1	D80564433ED35C850E2AD589B7713A4DAC01A09292869BDBB80E42E23F9336EA	5/13/2010	5/12/2020
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at <a href="https://www.verisign.com/rpa">https://www.verisign.com/rpa</a> (c)10, CN=VeriSign Class 3 Extended Validation SGC CA - T1	6EDAD2261AA3D53BE0D6FF5FA71C34A34B253B0C637B35BF3E966540F78B631B	5/13/2010	5/12/2020
C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 3 MPKI Secure Server CA, CN=Oracle SSL CA	7F6889FFE8B02045E2CAC99A2F2EE4F4C2EED24934B6521872D34BF812671C4B	10/12/2010	10/11/2020
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Extended Validation SHA256 SSL CA	1F9B31F820929EBFA03117EC2B77BA6B0FB6ECC9E027682A559378DA311C54EF	4/9/2013	4/8/2023



## DIGICERT, INC. MANAGEMENT’S ASSERTION

DigiCert, Inc. (“DigiCert”) operates the Symantec Certification Authority (“CA”) for its CAs as enumerated in [Attachment B](#) and provides extended validation SSL (“EV SSL”) CA services.

DigiCert management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its EV SSL CA services at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, throughout the period November 1, 2018 to October 31, 2019, DigiCert has:

- disclosed its EV SSL certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement for Symantec Trust Network (STN) and DigiCert Certificate Policy for Symantec Trust Network (STN) enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#).

DigiCert has disclosed the following matters publicly on Mozilla’s Bugzilla platform:

Mozilla Bug #	Description	Date Opened	Date Closed
<a href="#">Bugzilla 1515564</a>	DigiCert: Underscore character certificates	12/19/18	12/21/18
<a href="#">Bugzilla 1515788</a>	DigiCert: Underscores - CVS Pharmacy	12/20/18	02/11/19
<a href="#">Bugzilla 1516453</a>	DigiCert: Underscores - Discover	12/26/18	02/14/19
<a href="#">Bugzilla 1516545</a>	DigiCert: Underscores - Verizon	12/27/18	03/03/19
<a href="#">Bugzilla 1516561</a>	DigiCert: Underscores - Canadian Imperial Bank of Commerce	12/27/18	02/26/19
<a href="#">Bugzilla 1516599</a>	DigiCert: Underscores - Ericsson	12/27/18	05/01/19
<a href="#">Bugzilla 1517617</a>	DigiCert: Underscores - Citi	01/03/19	05/01/19
<a href="#">Bugzilla 1518555</a>	DigiCert: Use of forbidden subjectPublicKeyInfo algorithm	01/08/19	01/15/19
<a href="#">Bugzilla 1519572</a>	DigiCert: Underscores - Intuit	01/11/19	05/01/19
<a href="#">Bugzilla 1523676</a>	DigiCert: Good OCSP Responses for Revoked Intermediates	01/29/19	04/04/19
<a href="#">Bugzilla 1524875</a>	DigiCert: IP in dnsName	02/03/19	05/17/19
<a href="#">Bugzilla 1526154</a>	DigiCert: Missed Underscore Certificate Revocations	02/07/19	04/25/19



<b>Mozilla Bug #</b>	<b>Description</b>	<b>Date Opened</b>	<b>Date Closed</b>
<a href="#">Bugzilla 1527423</a>	DigiCert: P-384,ecdsa-with-SHA512 Certificates	02/12/19	07/18/19
<a href="#">Bugzilla 1531817</a>	DigiCert: in-addr.arpa Misissuance	03/01/19	07/01/19
<a href="#">Bugzilla 1533655</a>	DigiCert: Apple: Non-compliant Serial Numbers	03/07/19	07/20/19
<a href="#">Bugzilla 1539296</a>	DigiCert: KPN Outdated Audit	03/26/19	06/29/19
<a href="#">Bugzilla 1548716</a>	DigiCert: Verizon: "Default City" in Subject:localityName	05/02/19	05/20/19
<a href="#">Bugzilla 1548719</a>	DigiCert: Revoked intermediate certificates not in CRL	05/02/19	08/06/19
<a href="#">Bugzilla 1550645</a>	Digicert: CAA Checking Issue	05/09/19	Open as of report date
<a href="#">Bugzilla 1551363</a>	DigiCert: "Some-State" in stateOrProvinceName	05/13/19	09/06/19
<a href="#">Bugzilla 1556906</a>	DigiCert: Apple: Non-compliant Common Name Length	06/04/19	12/24/19
<a href="#">Bugzilla 1556948</a>	DigiCert Validation Scope Incident	06/04/19	11/26/19
<a href="#">Bugzilla 1563573</a>	DigiCert: Failure to disclose Unconstrained Intermediate within 7 Days	07/04/19	Open as of report date
<a href="#">Bugzilla 1566162</a>	DigiCert: Failure to supervise ABB Subordinate CA	07/15/19	09/15/19
<a href="#">Bugzilla 1573937</a>	DigiCert/Verizon: Qualified 2019 Audit Statements	08/14/19	Open as of report date
<a href="#">Bugzilla 1575125</a>	DigiCert: Apple: Unconstrained CAs not included in WTBR report	08/19/19	10/18/19
<a href="#">Bugzilla 1576013</a>	DigiCert: JOI Issue	08/22/19	Open as of report date
<a href="#">Bugzilla 1577014</a>	DigiCert OCSP services returns 1 byte	08/27/19	10/22/19
<a href="#">Bugzilla 1582519</a>	DigiCert: Apple: Precertificates without corresponding certificates return OCSP value of "unknown"	09/19/19	10/05/19
<a href="#">Bugzilla 1586604</a>	DigiCert: TERENA: No localityName in EV precert	10/06/19	10/08/19
<a href="#">Bugzilla 1593814</a>	DigiCert: & character in a printableString in ICA	11/04/19	12/24/19
<a href="#">Bugzilla 1595921</a>	DigiCert: Domain validation skipped	11/12/19	Open as of report date
<a href="#">Bugzilla 1596931</a>	DigiCert: Verizon CPS lacks problem reporting instructions	11/15/19	12/03/19



DigiCert, Inc.

A handwritten signature in black ink, appearing to read 'Dan Timpson', on a light gray rectangular background.

---

Dan Timpson  
Chief Technology Officer

January 29, 2020



## Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
<a href="#">DigiCert Certification Practices Statement for Symantec Trust Network (STN)</a>	3.13	June 25, 2019
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.12	April 18, 2019
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.11	March 18, 2019
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.10	November 2, 2018
DigiCert Certification Practices Statement for Symantec Trust Network (STN)	3.9	September 11, 2018
<a href="#">DigiCert Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018



## Attachment B - List of CAs In-Scope

Root CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
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	69DDD7EA90BB57C93E135DC85EA6FCD5480B603239BDC454FC758B2A26CF7F79	11/5/2007	1/18/2038
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Public Primary Certification Authority - G6	B32396746453442F353E616292BB20BBAA5D23B546450FDB9C54B8386167D529	10/18/2012	12/1/2037
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	2399561127A57125DE8CEFEA610DDF2FA078B5C8067F4E828290BFB860E84B3C	4/2/2008	12/1/2037
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	9ACFAB7E43C8D880D06B262A94DEEEE4B4659989C3D0CAF19BAF6405E41AB7DF	11/8/2006	7/16/2036
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Public Primary Certification Authority - G4	53DFDFA4E297FCFE07594E8C62D5B8AB06B32C7549F38A163094FD6429D5DA43	10/18/2012	12/1/2037
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Web PKI ECC Root - G1	92BB72F15EB75DE467C84B438181034BDAE9A016EC26434BEE3C9BBAD8CD8AF0	9/21/2017	9/20/2042
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Web PKI RSA Root - G1	F6BB5B7985A8736594C14679FA31603814502AAEB5F4282A69985DC84A450777	9/21/2017	9/20/2042

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G2	6C66B76E68D6C79FAFE5C94E9B7D0CF753C715CC85387E11323B7935F861C187	10/31/2013	10/30/2023
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3	9E6BC5F9ECC52460E8EDC02C644D1BE1CB9F2316F41DAF3B616A0B2058294B31	10/31/2013	10/30/2023





Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL SGC CA - G2	B2745D0A9B71D948F34E921AF59F342ADF6E407D88BC51D38AC52B583A0EBD15	10/31/2013	10/30/2023
C=US, O=Wells Fargo, OU=Symantec Trust Network, CN=Wells Fargo Certificate Authority WS1	C21087416BBF983B9FFE40F5D56EE0FFD94EB1E666B04A532ADE482EC201D67C	8/25/2015	8/24/2025
C=US, O=Oracle Corporation, OU=Symantec Trust Network, CN=Oracle SSL CA - G2	E4AF2FAE41187D58F209B01B1D8753C2DCCB3F601CE86273E37E8738C2A5CCB5	1/6/2015	1/5/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G4	31862233620E789330CC893E8B5E66705331B8B88B0ED30A44574D9E0A71C4F1	1/7/2016	1/6/2026
C=NZ, O=IBM New Zealand Limited, OU=Symantec Trust Network, CN=IBM New Zealand Limited Public CA	A6AE7959A195749CA887386FA04482BD169DC1157E312D301B0D5C333FAF2B02	2/3/2015	2/2/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit EV CA - G2	663636C03FD0B5B171F2B04407C3DF767B349C8A990D87CE485898166E2B5120	5/12/2015	5/11/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit Extended Validation CA	5AD4183B54F0E2762DA8D910E1E7E9F2AB2F1BC4CE6A638F0DBBF337EB4A139F	12/20/2012	12/19/2022
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit EV CA - G3	4B2CBA18EFBCE6C3C4A80AAABC952337000CD9346B768D062412A2DED846EDC9	1/7/2016	1/6/2026
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 384 bit Extended Validation CA	77FE876A1C476349F5EB9AE9BF53F7814A0AE411562667C58B7ED27869C54091	12/20/2012	12/19/2022



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at <a href="https://www.verisign.com/rpa">https://www.verisign.com/rpa</a> (c)10, CN=VeriSign Class 3 Extended Validation CA - T1	D80564433ED35C850E2AD589B7713A4DAC01A09292869BDBB80E42E23F9336EA	5/13/2010	5/12/2020
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at <a href="https://www.verisign.com/rpa">https://www.verisign.com/rpa</a> (c)10, CN=VeriSign Class 3 Extended Validation SGC CA - T1	6EDAD2261AA3D53BE0D6FF5FA71C34A34B253B0C637B35BF3E966540F78B631B	5/13/2010	5/12/2020
C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 3 MPKI Secure Server CA, CN=Oracle SSL CA	7F6889FFE8B02045E2CAC99A2F2EE4F4C2EED24934B6521872D34BF812671C4B	10/12/2010	10/11/2020
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Extended Validation SHA256 SSL CA	1F9B31F820929EBFA03117EC2B77BA6B0FB6ECC9E027682A559378DA311C54EF	4/9/2013	4/8/2023



Tel: 314-889-1100

Fax: 314-889-1101

[www.bdo.com](http://www.bdo.com)

101 S Hanley Rd, #800

St. Louis, MO 63105

## REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of DigiCert, Inc. (“DigiCert”):

We have examined DigiCert management’s [assertion](#) that for its GeoTrust Certification Authority (“CA”) operations at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, throughout the period November 1, 2018 to October 31, 2019 for CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement for GeoTrust and RapidSSL and DigiCert Certificate Policy for Symantec Trust Network (STN) enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#). DigiCert’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

The relative effectiveness and significance of specific controls at DigiCert 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 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 management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.



Because of the nature and inherent limitations of controls, DigiCert'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 management's assertion, as referred to above, is fairly stated, in all material respects.

We did not note any instances of possible non-conformance relevant to the CAs enumerated in [Attachment B](#). DigiCert's assertion notes all instances possible non-conformance, addressed by DigiCert, during the engagement period, regardless of the particular CAs enumerated in [Attachment B](#).

This report does not include any representation as to the quality of DigiCert's services other than its GeoTrust CA operations at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, nor the suitability of any of DigiCert's services for any customer's intended purpose.

DigiCert'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

January 29, 2020



## Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
<a href="#">DigiCert Certification Practices Statement for GeoTrust and RapidSSL</a>	1.6	June 25, 2019
DigiCert Certification Practices Statement for GeoTrust and RapidSSL	1.5	April 18, 2019
DigiCert Certification Practices Statement for GeoTrust and RapidSSL	1.4	March 18, 2019
DigiCert Certification Practices Statement for GeoTrust and RapidSSL	1.3	November 2, 2018
DigiCert Certification Practices Statement for GeoTrust, RapidSSL, and FreeSSL	1.2	September 11, 2018
<a href="#">DigiCert Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018



## Attachment B - List of CAs In-Scope

Root CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., OU=(c) 2008 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification Authority - G3	B478B812250DF878635C2AA7EC7D155EAA625EE82916E2CD294361886CD1FBD4	4/2/2008	12/1/2037
C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority	37D51006C512EAAB626421F1EC8C92013FC5F82AE98EE533EB4619B8DEB4D06C	11/27/2006	7/16/2036
C=US, O=GeoTrust Inc., OU=(c) 2007 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification Authority - G2	5EDB7AC43B82A06A8761E8D7BE4979EBF2611F7DD79BF91C1C6B566A219ED766	11/5/2007	1/18/2038

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G4	95B09D02122FA8AE6235780F6EA6503E767AC021A0874FE831CE803A50EA8FD7	10/31/2013	10/30/2023
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G5	5B2AE8ABF5E7E563BBC34C97A22554E82393D7ACC09C1765E504AE08C157B5AC	9/9/2014	9/8/2024
C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SHA256 SSL CA	BC9E223CC42275CC034190DF2D0179B55B732D5AC531137A7B522DCFE04A0592	4/9/2013	4/8/2023



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SSL CA - G2	C7B57A02F937AE0BE3E21027030592C9D47A70D7013EB3AA94DBC3B7B5AB0662	8/23/2012	8/22/2022
C=US, O=GeoTrust, Inc., CN=GeoTrust ECC EV SSL CA	C131499FD86B213DB5DEFAAFD53111C28A2DDAF4BA465C8265A72D6CF739B668	1/7/2016	1/6/2026
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G6	419B0C9AD6B872A8B1BB87341AF63EE92E69B27B996662E733032F1288108DFB	5/1/2017	4/29/2027
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G7	546CAFF9060EEF30F4F3E02255FBF5131E657C1710C9A650020133A818BEC1C8	5/1/2017	4/29/2027



## DIGICERT, INC. MANAGEMENT’S ASSERTION

DigiCert, Inc. (“DigiCert”) operates the GeoTrust Certification Authority (“CA”) for its CAs as enumerated in [Attachment B](#) and provides extended validation SSL (“EV SSL”) CA services.

DigiCert management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its EV SSL CA services at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, throughout the period November 1, 2018 to October 31, 2019, DigiCert has:

- disclosed its EV SSL certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement for GeoTrust and RapidSSL and DigiCert Certificate Policy for Symantec Trust Network (STN) enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#).

DigiCert has disclosed the following matters publicly on Mozilla’s Bugzilla platform:

Mozilla Bug #	Description	Date Opened	Date Closed
<a href="#">Bugzilla 1515564</a>	DigiCert: Underscore character certificates	12/19/18	12/21/18
<a href="#">Bugzilla 1515788</a>	DigiCert: Underscores - CVS Pharmacy	12/20/18	02/11/19
<a href="#">Bugzilla 1516453</a>	DigiCert: Underscores - Discover	12/26/18	02/14/19
<a href="#">Bugzilla 1516545</a>	DigiCert: Underscores - Verizon	12/27/18	03/03/19
<a href="#">Bugzilla 1516561</a>	DigiCert: Underscores - Canadian Imperial Bank of Commerce	12/27/18	02/26/19
<a href="#">Bugzilla 1516599</a>	DigiCert: Underscores - Ericsson	12/27/18	05/01/19
<a href="#">Bugzilla 1517617</a>	DigiCert: Underscores - Citi	01/03/19	05/01/19
<a href="#">Bugzilla 1518555</a>	DigiCert: Use of forbidden subjectPublicKeyInfo algorithm	01/08/19	01/15/19
<a href="#">Bugzilla 1519572</a>	DigiCert: Underscores - Intuit	01/11/19	05/01/19
<a href="#">Bugzilla 1523676</a>	DigiCert: Good OCSP Responses for Revoked Intermediates	01/29/19	04/04/19
<a href="#">Bugzilla 1524875</a>	DigiCert: IP in dnsName	02/03/19	05/17/19





Mozilla Bug #	Description	Date Opened	Date Closed
<a href="#">Bugzilla 1526154</a>	DigiCert: Missed Underscore Certificate Revocations	02/07/19	04/25/19
<a href="#">Bugzilla 1527423</a>	DigiCert: P-384,ecdsa-with-SHA512 Certificates	02/12/19	07/18/19
<a href="#">Bugzilla 1531817</a>	DigiCert: in-addr.arpa Misissuance	03/01/19	07/01/19
<a href="#">Bugzilla 1533655</a>	DigiCert: Apple: Non-compliant Serial Numbers	03/07/19	07/20/19
<a href="#">Bugzilla 1539296</a>	DigiCert: KPN Outdated Audit	03/26/19	06/29/19
<a href="#">Bugzilla 1548716</a>	DigiCert: Verizon: "Default City" in Subject:localityName	05/02/19	05/20/19
<a href="#">Bugzilla 1548719</a>	DigiCert: Revoked intermediate certificates not in CRL	05/02/19	08/06/19
<a href="#">Bugzilla 1550645</a>	Digicert: CAA Checking Issue	05/09/19	Open as of report date
<a href="#">Bugzilla 1551363</a>	DigiCert: "Some-State" in stateOrProvinceName	05/13/19	09/06/19
<a href="#">Bugzilla 1556906</a>	DigiCert: Apple: Non-compliant Common Name Length	06/04/19	12/24/19
<a href="#">Bugzilla 1556948</a>	DigiCert Validation Scope Incident	06/04/19	11/26/19
<a href="#">Bugzilla 1563573</a>	DigiCert: Failure to disclose Unconstrained Intermediate within 7 Days	07/04/19	Open as of report date
<a href="#">Bugzilla 1566162</a>	DigiCert: Failure to supervise ABB Subordinate CA	07/15/19	09/15/19
<a href="#">Bugzilla 1573937</a>	DigiCert/Verizon: Qualified 2019 Audit Statements	08/14/19	Open as of report date
<a href="#">Bugzilla 1575125</a>	DigiCert: Apple: Unconstrained CAs not included in WTBR report	08/19/19	10/18/19
<a href="#">Bugzilla 1576013</a>	DigiCert: JOI Issue	08/22/19	Open as of report date
<a href="#">Bugzilla 1577014</a>	DigiCert OCSP services returns 1 byte	08/27/19	10/22/19
<a href="#">Bugzilla 1582519</a>	DigiCert: Apple: Precertificates without corresponding certificates return OCSP value of "unknown"	09/19/19	10/05/19
<a href="#">Bugzilla 1586604</a>	DigiCert: TERENA: No localityName in EV precert	10/06/19	10/08/19
<a href="#">Bugzilla 1593814</a>	DigiCert: & character in a printableString in ICA	11/04/19	12/24/19
<a href="#">Bugzilla 1595921</a>	DigiCert: Domain validation skipped	11/12/19	Open as of report date
<a href="#">Bugzilla 1596931</a>	DigiCert: Verizon CPS lacks problem reporting instructions	11/15/19	12/03/19



DigiCert, Inc.

A handwritten signature in black ink, appearing to read 'Dan Timpson', on a light gray rectangular background.

---

Dan Timpson  
Chief Technology Officer

January 29, 2020



## Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
<a href="#">DigiCert Certification Practices Statement for GeoTrust and RapidSSL</a>	1.6	June 25, 2019
DigiCert Certification Practices Statement for GeoTrust and RapidSSL	1.5	April 18, 2019
DigiCert Certification Practices Statement for GeoTrust and RapidSSL	1.4	March 18, 2019
DigiCert Certification Practices Statement for GeoTrust and RapidSSL	1.3	November 2, 2018
DigiCert Certification Practices Statement for GeoTrust, RapidSSL, and FreeSSL	1.2	September 11, 2018
<a href="#">DigiCert Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018



## Attachment B - List of CAs In-Scope

Root CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., OU=(c) 2008 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification Authority - G3	B478B812250DF878635C2AA7EC7D155EAA625EE82916E2CD294361886CD1FBD4	4/2/2008	12/1/2037
C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority	37D51006C512EAA8626421F1EC8C92013FC5F82AE98EE533EB4619B8DEB4D06C	11/27/2006	7/16/2036
C=US, O=GeoTrust Inc., OU=(c) 2007 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification Authority - G2	5EDB7AC43B82A06A8761E8D7BE4979EBF2611F7DD79BF91C1C6B566A219ED766	11/5/2007	1/18/2038

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G4	95B09D02122FA8AE6235780F6EA6503E767AC021A0874FE831CE803A50EA8FD7	10/31/2013	10/30/2023
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G5	5B2AE8ABF5E7E563BBC34C97A22554E82393D7ACC09C1765E504AE08C157B5AC	9/9/2014	9/8/2024
C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SHA256 SSL CA	BC9E223CC42275CC034190DF2D0179B55B732D5AC531137A7B522DCFE04A0592	4/9/2013	4/8/2023



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SSL CA - G2	C7B57A02F937AE0BE3E21027030592C9D47A70D7013EB3AA94DBC3B7B5AB0662	8/23/2012	8/22/2022
C=US, O=GeoTrust, Inc., CN=GeoTrust ECC EV SSL CA	C131499FD86B213DB5DEFAAFD53111C28A2DDAF4BA465C8265A72D6CF739B668	1/7/2016	1/6/2026
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G6	419B0C9AD6B872A8B1BB87341AF63EE92E69B27B996662E733032F1288108DFB	5/1/2017	4/29/2027
C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G7	546CAFF9060EEF30F4F3E02255FBF5131E657C1710C9A650020133A818BEC1C8	5/1/2017	4/29/2027



Tel: 314-889-1100  
Fax: 314-889-1101  
[www.bdo.com](http://www.bdo.com)

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

## REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of DigiCert, Inc. (“DigiCert”):

We have examined DigiCert management’s [assertion](#) that for its Thawte Certification Authority (“CA”) operations at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, throughout the period November 1, 2018 to October 31, 2019 for CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement for Thawte-Branded Certificates and DigiCert Certificate Policy for Symantec Trust Network (STN) enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#). DigiCert’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

The relative effectiveness and significance of specific controls at DigiCert 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 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 management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.



Because of the nature and inherent limitations of controls, DigiCert'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 management's assertion, as referred to above, is fairly stated, in all material respects.

We did not note any instances of possible non-conformance relevant to the CAs enumerated in [Attachment B](#). DigiCert's assertion notes all instances possible non-conformance, addressed by DigiCert, during the engagement period, regardless of the particular CAs enumerated in [Attachment B](#).

This report does not include any representation as to the quality of DigiCert's services other than its Thawte CA operations at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, nor the suitability of any of DigiCert's services for any customer's intended purpose.

DigiCert'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

January 29, 2020



## Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
<a href="#">DigiCert Certification Practices Statement for Thawte-Branded Certificates</a>	3.7.23	June 25, 2019
DigiCert Certification Practices Statement for Thawte-Branded Certificates	3.7.22	April 18, 2019
DigiCert Certification Practices Statement for Thawte-Branded Certificates	3.7.21	March 18, 2019
DigiCert Certification Practices Statement for Thawte-Branded Certificates	3.7.20	November 2, 2018
DigiCert Certification Practices Statement for Thawte	3.7.19	September 11, 2018
<a href="#">DigiCert Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018





## Attachment B - List of CAs In-Scope

Root CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	8D722F81A9C113C0791DF136A2966DB26C950A971DB46B4199F4EA54B78BFB9F	11/17/2006	7/16/2036
C=US, O=thawte, Inc., OU=(c) 2007 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G2	A4310D50AF18A6447190372A86AF8B951FFB431D837F1E5688B45971ED1557	11/5/2007	1/18/2038
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2008 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G3	4B03F45807AD70F21BFC2CAE71C9FDE4604C064CF5FFB686BAE5DBAAD7FDD34C	4/2/2008	12/1/2037

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., CN=thawte ECC EV SSL CA	EAD62F42BB369DD43CF6131AC2D8D72E4F9FEE85E69D45DAAFFE326AAC2A46F1	1/7/2016	1/6/2026
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G2	37F6BD9BEE0C74F608DD474B56A72F8183077DFC2662AF79BFE3D4FABCF0B1C4	10/31/2013	10/30/2023
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G3	1A99019F9D412A64454749EDAA8E7DC46673D644DF3CE15CC655735EA0DF86FE	10/31/2013	10/30/2023



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., CN=thawte Extended Validation SHA256 SSL CA	7920B8E18D2FC12D81C2FAB90A63B1B52AB329CE7CD1CB7CA094CDF9D600F492	4/9/2013	4/8/2023



## DIGICERT, INC. MANAGEMENT’S ASSERTION

DigiCert, Inc. (“DigiCert”) operates the Thawte Certification Authority (“CA”) for its CAs as enumerated in [Attachment B](#) and provides extended validation SSL (“EV SSL”) CA services.

DigiCert management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its EV SSL CA services at various locations in the United States of America, Australia, South Africa, Ireland, and Japan, throughout the period November 1, 2018 to October 31, 2019, DigiCert has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certification Practices Statement for Thawte-Branded Certificates and DigiCert Certificate Policy for Symantec Trust Network (STN) enumerated in [Attachment A](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its [website](#), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated

based on the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2](#).

DigiCert has disclosed the following matters publicly on Mozilla’s Bugzilla platform:

Mozilla Bug #	Description	Date Opened	Date Closed
<a href="#">Bugzilla 1515564</a>	DigiCert: Underscore character certificates	12/19/18	12/21/18
<a href="#">Bugzilla 1515788</a>	DigiCert: Underscores - CVS Pharmacy	12/20/18	02/11/19
<a href="#">Bugzilla 1516453</a>	DigiCert: Underscores - Discover	12/26/18	02/14/19
<a href="#">Bugzilla 1516545</a>	DigiCert: Underscores - Verizon	12/27/18	03/03/19
<a href="#">Bugzilla 1516561</a>	DigiCert: Underscores - Canadian Imperial Bank of Commerce	12/27/18	02/26/19
<a href="#">Bugzilla 1516599</a>	DigiCert: Underscores - Ericsson	12/27/18	05/01/19
<a href="#">Bugzilla 1517617</a>	DigiCert: Underscores - Citi	01/03/19	05/01/19
<a href="#">Bugzilla 1518555</a>	DigiCert: Use of forbidden subjectPublicKeyInfo algorithm	01/08/19	01/15/19
<a href="#">Bugzilla 1519572</a>	DigiCert: Underscores - Intuit	01/11/19	05/01/19
<a href="#">Bugzilla 1523676</a>	DigiCert: Good OCSP Responses for Revoked Intermediates	01/29/19	04/04/19
<a href="#">Bugzilla 1524875</a>	DigiCert: IP in dnsName	02/03/19	05/17/19



Mozilla Bug #	Description	Date Opened	Date Closed
<a href="#">Bugzilla 1526154</a>	DigiCert: Missed Underscore Certificate Revocations	02/07/19	04/25/19
<a href="#">Bugzilla 1527423</a>	DigiCert: P-384,ecdsa-with-SHA512 Certificates	02/12/19	07/18/19
<a href="#">Bugzilla 1531817</a>	DigiCert: in-addr.arpa Misissuance	03/01/19	07/01/19
<a href="#">Bugzilla 1533655</a>	DigiCert: Apple: Non-compliant Serial Numbers	03/07/19	07/20/19
<a href="#">Bugzilla 1539296</a>	DigiCert: KPN Outdated Audit	03/26/19	06/29/19
<a href="#">Bugzilla 1548716</a>	DigiCert: Verizon: "Default City" in Subject:localityName	05/02/19	05/20/19
<a href="#">Bugzilla 1548719</a>	DigiCert: Revoked intermediate certificates not in CRL	05/02/19	08/06/19
<a href="#">Bugzilla 1550645</a>	Digicert: CAA Checking Issue	05/09/19	Open as of report date
<a href="#">Bugzilla 1551363</a>	DigiCert: "Some-State" in stateOrProvinceName	05/13/19	09/06/19
<a href="#">Bugzilla 1556906</a>	DigiCert: Apple: Non-compliant Common Name Length	06/04/19	12/24/19
<a href="#">Bugzilla 1556948</a>	DigiCert Validation Scope Incident	06/04/19	11/26/19
<a href="#">Bugzilla 1563573</a>	DigiCert: Failure to disclose Unconstrained Intermediate within 7 Days	07/04/19	Open as of report date
<a href="#">Bugzilla 1566162</a>	DigiCert: Failure to supervise ABB Subordinate CA	07/15/19	09/15/19
<a href="#">Bugzilla 1573937</a>	DigiCert/Verizon: Qualified 2019 Audit Statements	08/14/19	Open as of report date
<a href="#">Bugzilla 1575125</a>	DigiCert: Apple: Unconstrained CAs not included in WTBR report	08/19/19	10/18/19
<a href="#">Bugzilla 1576013</a>	DigiCert: JOI Issue	08/22/19	Open as of report date
<a href="#">Bugzilla 1577014</a>	DigiCert OCSP services returns 1 byte	08/27/19	10/22/19
<a href="#">Bugzilla 1582519</a>	DigiCert: Apple: Precertificates without corresponding certificates return OCSP value of "unknown"	09/19/19	10/05/19
<a href="#">Bugzilla 1586604</a>	DigiCert: TERENA: No localityName in EV precert	10/06/19	10/08/19
<a href="#">Bugzilla 1593814</a>	DigiCert: & character in a printableString in ICA	11/04/19	12/24/19
<a href="#">Bugzilla 1595921</a>	DigiCert: Domain validation skipped	11/12/19	Open as of report date
<a href="#">Bugzilla 1596931</a>	DigiCert: Verizon CPS lacks problem reporting instructions	11/15/19	12/03/19



DigiCert, Inc.

A handwritten signature in black ink, appearing to read 'Dan Timpson', is placed on a light gray rectangular background.

---

Dan Timpson  
Chief Technology Officer

January 29, 2020



**Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope**

<b>Policy Name</b>	<b>Version</b>	<b>Date</b>
<a href="#">DigiCert Certification Practices Statement for Thawte-Branded Certificates</a>	3.7.23	June 25, 2019
DigiCert Certification Practices Statement for Thawte-Branded Certificates	3.7.22	April 18, 2019
DigiCert Certification Practices Statement for Thawte-Branded Certificates	3.7.21	March 18, 2019
DigiCert Certification Practices Statement for Thawte-Branded Certificates	3.7.20	November 2, 2018
DigiCert Certification Practices Statement for Thawte	3.7.19	September 11, 2018
<a href="#">DigiCert Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018



## Attachment B - List of CAs In-Scope

Root CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	8D722F81A9C113C0791DF136A2966DB26C950A971DB46B4199F4EA54B78BFB9F	11/17/2006	7/16/2036
C=US, O=thawte, Inc., OU=(c) 2007 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G2	A4310D50AF18A6447190372A86AF8B951FFB431D837F1E5688B45971ED1557	11/5/2007	1/18/2038
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2008 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G3	4B03F45807AD70F21BFC2CAE71C9FDE4604C064CF5FFB686BAE5DBAAD7FDD34C	4/2/2008	12/1/2037

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., CN=thawte ECC EV SSL CA	EAD62F42BB369DD43CF6131AC2D8D72E4F9FEE85E69D45DAAFFE326AAC2A46F1	1/7/2016	1/6/2026
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G2	37F6BD9BEE0C74F608DD474B56A72F8183077DFC2662AF79BFE3D4FABCF0B1C4	10/31/2013	10/30/2023
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G3	1A99019F9D412A64454749EDAA8E7DC46673D644DF3CE15CC655735EA0DF86FE	10/31/2013	10/30/2023
C=US, O=thawte, Inc., CN=thawte Extended Validation SHA256 SSL CA	7920B8E18D2FC12D81C2FAB90A63B1B52AB329CE7CD1CB7CA094CDF9D600F492	4/9/2013	4/8/2023