



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

101 South Hanley Road, Suite 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 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 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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#). 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 judgement, 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 matter during our procedures:

Matter Topic		Matter Description
1	Certificate Request Validation and Certificate Revocation	DigiCert disclosed in <a href="#">Mozilla Bug 1550645</a> that CAA record checking resulted in an approval when the service request timed out. This could have led to a certificate being issued, despite the fact a CAA check would have failed. In total, 1,053 active certificates were discovered to have been issued under these circumstances. DigiCert did not revoke all the certificates impacted by these circumstances in the timelines required by the Baseline Requirements.
		DigiCert disclosed in <a href="#">Mozilla Bug 1556948</a> that a system error allowed base domains, which were not validated, to be added to certificates with properly validated subdomains. An internal investigation was launched and resulted in the discovery of 1,069 certificates having been issued with under these circumstances.
2	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> .



		DigiCert disclosed the Mozilla Bugs listed below certificates were issued with underscore characters in the dNSName, which violates RFC 5280. DigiCert did not revoke all of the certificates impacted by these circumstances in the timelines required by the Baseline Requirements. - <a href="#">Mozilla Bug 1516599</a> - <a href="#">Mozilla Bug 1517617</a> - <a href="#">Mozilla Bug 1519572</a>
3	Certificate Status Validation	DigiCert was notified in <a href="#">Mozilla Bug 1577014</a> its OCSP responder was returning a one (1) byte, unsigned, response when requested for the status of a certificate serial number that was not issued, but for which a pre-certificate was created.
4	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.
5	System Access Reviews	System access reviews were performed at the network and physical access levels. For the first three quarters of the engagement period, access reviews did not include application level access or offline systems in the scope of the review.

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 - SSL Baseline with Network Security 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	802447EE521CC666CDB7BBAE93A385E55F200D76A3D1356A85445AC4CDBED12	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
Hotspot 2.0 Trust Root CA - 03	A3CC68595DFE7E86D8AD1772A8B5284ADD54ACE3B8A798DF47BCCAFB1FDB84DF	12/8/2013	12/8/2043
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



Cross-Signed Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Global Root CA	6DACBB8945137B1DAD4211B0436EFBE06F12ACE36904973B45AE25740823D369	12/7/2016	5/10/2025
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
AAMC Direct Intermediate CA	BB1C01E884DD0919AB94D5AF5575CD6FEB71E560B2B58735A78B150A10D54BF3	5/28/2015	5/28/2025
Abbott Laboratories Secure Authentication CA	DB99A4F284CCF10B26DE7B7A5D651725B857CBC871EBB33028D67B55510EFC9	8/23/2016	8/23/2026
Abbott Laboratories Secure Server CA	6C69E201656440EB98CD0875764A1ED19015ED8C4427601ACA9C68AFA8973959	7/12/2016	7/12/2026
Adobe Analytics - DigiCert CA	D5C009312F845C5EC8506EAD560D62447BFF4A60A9C25210511217AD6DE76AED	4/18/2013	4/18/2021
Aetna Inc. Secure CA2	5D28761CBF304EAFCD127B34D614FE179AC7744F1552AF1C31298425AD05A275	12/9/2014	12/9/2024
Aetna Inc. Secure EV CA	0A163600631BD66267FB7AEAD25C538B2B7D72AD6416A2BBD285F654BB642F6D	12/9/2014	12/9/2024
Aetna Inc. Secure EV CA2	1DDFDDF883E3945B2CB24FA5B83788379C5AB058422AB979DF66C77473988687	12/8/2017	12/8/2027
Alaska eHealth Network CA	437859303D0183862A96F6ABF8B03F2A69D4CBD317217666015E1ABA3C84AA11	10/22/2013	10/22/2023
Allina Health Connect HIE Intermediate CA	826C6AA610EF190BE2D7C03E22D032405B289804E3319E233C4C37FFBF305F1A	12/8/2015	12/8/2025
Amazon Server CA 1B	4A1FF6BBF481170D3B773CEC1F3A84DE3B5096575CDBF8B08432209318CA0FBD	10/21/2015	10/21/2040
Amazon Server CA 1B	F55F9FFCB83C73453261601C7E044DB15A0F034B93C05830F28635EF889CF670	10/22/2015	10/22/2025



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Axesson Direct CA	BF4655F16AA338D7C7FF2BDC949A524BD4797B8B3C8341C608C9F65CB1CB8177	1/8/2014	1/8/2024
Cal INDEX CA	A5226F33474B53392665298B48F4E6129824E98BD4D38DF4E31EBBCF14FA33CD	7/12/2016	7/12/2026
Care360 Direct Intermediate CA	2D602B1F166D6316DAFD46B4B1EDD6DCFC54D2AF8A944BE358858FD504AAA16B	8/25/2015	8/25/2025
Catholic Health Initiatives CA	151A3591B765D02C359EEC9C56ED8DDAD0C54E756A497D02BF979FA8DD5D95BB	8/19/2014	8/19/2024
Cerner Corporation Direct Intermediate CA	09DE7FA739EE47C06291845F2E0E8A9E1C7CC2900AD354CF167316E02386BD9B	9/26/2014	9/26/2024
Cerner Corporation Resonance Intermediate CA	64284AA5F8DC8697D43D9737CF4E266625414E449C019667714537FF7EDE31B7	11/11/2015	11/11/2021
Cisco Meraki CA	199EE58009555DAE2CDA0626931C64391D6A88CCCB1F9F0B2EE80B667F581C06	7/12/2016	7/12/2026
CloudFlare Inc ECC CA-2	6172D7A1996CBEF71A0182DD44B99E9C035742A9EBD0311AA73AA4733344C5A6	10/14/2015	10/9/2020
CloudFlare Inc RSA CA-1	328C5991D8383E27D0EBE910BF66C0AF3D748A85D3011A52D88F1D8C8635647F	10/14/2015	10/14/2020
CompuGroup Medical Certificate Authority	B604026A3590392ABEFB6B18E8176453656115D2A0060F713E191A9FD076532A	12/8/2015	12/8/2025
Corepoint Direct Intermediate CA	CD2640957CF88610470CEFD409D85D9BE05962F7D6C2999C4F431ABCCC34118C	1/14/2015	1/14/2025
Cybertrust Japan ECC EV CA	92E3770B1EB44F84C2F2CB0097C2FD7126BD212B41C2610E78DDFD8946761738	8/24/2017	8/24/2032
Cybertrust Japan Extended Validation Server CA	0E10BDDEE7512DBD79EBF0B4F48FEED7C83C2BD3DD81765565F4FF110B7BFA42	12/7/2016	12/7/2031
Cybertrust Japan Issuing CA-1	87942388D29A46C06FE1E56AAB791594D0FB2E8EABF124048F130EEA9BEDD3FD	9/1/2016	9/1/2026
Cybertrust Japan Secure Server CA	33D57359831F87754E6E755D6B5B56E7E71297DDDFEA1D6397086604280F6FFC	12/7/2016	12/7/2031
Cybertrust Japan Secure Server ECC CA	C3683F7D91754219DADA4E8DC30E4B18BD3928B53D3AB93D07384BC5871CE355	7/13/2017	7/13/2032
Data Management Intermediate Certificate Authority	54837EF7B5AC4AA23606A15EF30DE46E9BB7E23E60F6ED4F2612092B94EDC68F	8/25/2015	8/25/2025
DC Government SHA2 Assured ID Intermediate CA	FB1147E7AB97A29BB9C1140ABF3DE831F4C5F60D11B90FEC999A0816375D8457	7/13/2017	7/13/2027
DC Government SHA2 EV Intermediate CA	F12241EE34C03A608D34DBC0EA465E1BD1AA13091554F9D4D086253FF3CE83D4	7/13/2017	7/13/2027
DigiCert Accredited Direct Med CA	0E78434EC8AD6613562C8390D8B3306FC6087E0593C7D5AC2FAF9AD263879745	8/6/2013	8/6/2023
DigiCert Assured ID CA G2	93C381CB07B353A920C2A7BED6BEBF195C68279DD0527D37F20BDD0D99C330FA	8/1/2013	8/1/2028
DigiCert Assured ID CA G3	634FDF26C994E76A2918D9EFC4CAB9C6FCB344EF642A79C89192BCDA0ED52F4C	8/1/2013	8/1/2028
DigiCert Assured ID CA-1	425E72C87FF2285D9908B71AB4C64B0D2F248287097690C62FE733F631DE38F	11/10/2006	11/10/2021



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Assured ID CA-1	B8F44E4B1F8697DF54BB3D0F1E67596CE2FE9DABA85AF4E6F2A2E74396F8C56D	11/10/2006	11/10/2021
DigiCert Assured ID Intermediate CA (SHA2)	C2B4BBEF4A1A643F334ED0850F928876D2AE3AE3642B986014D68C673C04D081	12/7/2011	12/7/2026
DigiCert Assured ID TLS CA	D7737E5F2D3FFCA429902E9F388CFD6C5959CD35A0FC103CEE2F7E93D1C66A52	2/9/2018	2/9/2030
DigiCert Baltimore CA-1 G2	BF1CB0E213D8D3C70BAE89429FC16DE2C74F755963D1B9B488BD0260DBC91B9C	10/14/2015	5/10/2025
DigiCert Baltimore CA-2 G2	F9690880819F06CDDCC0B2F224B207F2AF6003FB57339B8679A160FA95208D62D	12/8/2015	5/10/2025
DigiCert Baltimore EV CA	D46931E0182DD655EA0C16E6DD99F8E61AFFE401F734C6CA8EA0056A968EAF81	10/14/2015	5/10/2025
DigiCert Cloud Services CA-1	2F6889961A7CA7067E8BA103C2CF9B9A924F8CA293F11178E23A1978D2F133D3	8/4/2015	8/4/2030
DigiCert Direct Non-Provider CA	1AEDDADDC1ED748543EAF5960DF96AD51E21A3164F30A0640CB0732365D39062	2/11/2014	2/11/2024
DigiCert ECC Extended Validation Server CA	FDC8986CFAC4F35F1ACD517E0F61B879882AE076E2BA80B77BD3F0FE5CEF8862	6/21/2016	6/21/2031
DigiCert ECC Secure Server CA	458446BA75D932E914F23C2B57B7D192EDDBC2181D958E1181AD5251747A1EE8	3/8/2013	3/8/2023
DigiCert EV Server CA G4	710024B37BD9F0E1537C18A4C20F9A31C4B485D1248C643F20B4C00F3716BA85	1/17/2017	1/17/2032
DigiCert Extended Validation CA G3	7C0912E5DE8478BB86E8EA46BA5AE65DC3870BCEFCBC2F46795EEECF648CFBE7	11/11/2015	11/11/2030
DigiCert Extended Validation Intermediate CA (SHA2)	802C2AD1D215E57CDC9010EA437ACE399B657194FBD40E3BB5E00B080E6496DF	12/7/2011	12/7/2026
DigiCert Federated Healthcare CA	54C3F501042CDCC09AE8143CB192BD5E5724C9C88A6AB395A94A1A7AFC26CE7C	2/11/2014	2/11/2024
DigiCert Federated ID L1 CA	CAB016C5EA32061BD065FE13A55A40FA61058B27B34A7F8D175F7101EE063E3B	10/30/2012	10/30/2022
DigiCert Federated ID L2 CA	91FDEB52D4265120B843B195D1B6CDB5CE61251865A45A3E920E610FDDA660D3	1/7/2014	1/7/2023
DigiCert Federated ID L3 CA	85760F77DB0FD0D93C21EE0364B8EAB09B82CF49B7849831038209B5B1081363	1/7/2014	1/7/2023
DigiCert Federated ID L4 CA	EFB2A3F37273D3589047919825EA5337E9B938A8C178B61C18C2B4270B9665AC	10/30/2012	10/30/2022
DigiCert Federated ID US L3 CA	EB84FC0B403D9B689297A5D83EA186838E3B777BC618EFDA162A75B7FEA666C1	1/8/2014	1/8/2023
DigiCert Federated ID US L4 CA	6797436214EFEE67CDE7D70358D4D8B00DFBF78D5C87C62B4A7E90D73DD7BD9	4/18/2013	4/18/2023
DigiCert Federated Trust CA	E5BBDDCAD572EC9D2DD96E0E5EBF049A9181F070F1E33CC1635AD8EC487D2177	11/18/2011	11/18/2023
DigiCert Global CA G2	8FAC576439C9FD3EF153B51F9EDD0D381B5DF7B87559CEBECA04297DD44A639B	8/1/2013	8/1/2028
DigiCert Global CA G3	F7541CF69D1DE1AC953ABC1FAD6F7807A34EDFE9E12C11E66A195930C23AD6C6	8/1/2013	8/1/2028





Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Global CA-1	3C750409882486D64151F4CBB5BD61432A4A7BF42F48A85198D245A64AEA2117	11/10/2006	11/10/2021
DigiCert Governmental Direct CA	5F665CBACC1E37171EA83EA85C570F9861CAF77BAC8886ABC4BB19B3698C094A	9/25/2015	9/25/2025
DigiCert Grid Trust CA	1E0A3AB993157717281D42ABF801EB64DEED500EA4168CA706D6A71D8103C73A2	12/7/2011	12/7/2026
DigiCert Grid Trust CA G2	28CBB4E0D9C4EE6D04AC8F14717605AE3A4BD8CBF8D081B27AF6EDB2F3D76A32	1/8/2014	1/8/2029
DigiCert High Assurance CA-3	21EB37AB4CF6EF8965EC1766409CA76B8B2E03F2D1A388DF734208E86DEEE679	4/2/2008	4/3/2022
DigiCert High Assurance CA-3	57D8D5B832616B7823466A0C372770D16A5DCF246581F0F58373E51C7E1E5316	4/3/2007	4/3/2022
DigiCert High Assurance CA-3	COA4A1AC05E03096A3B2AB8A38502B39E2614E11397BEE73D0A66B8ACEF7A283	4/3/2008	4/3/2022
DigiCert High Assurance CA-3	DCB400ACC249FB8483415FC2650BC90488CA96643118CB0E4F4424B21C3AA5A4	10/12/2011	4/3/2022
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	8FC1469B8005BFE8BDF67F514E795FE1F17EA239A2A6934857F2428ADCE6D24F	11/10/2007	11/10/2021
DigiCert High Assurance EV CA-2	1188F831C949A62E9C9D4F60E36F72544F0AF924DE07F9DA992E26E44C996EEE0	3/23/2007	3/23/2022
DigiCert High Assurance Intermediate CA (SHA2)	47511629F2BC3B7CF84EFEC9F32798A43AF6252E550B6CAE76A38558712E37D8	12/7/2011	12/7/2026
DigiCert Provisional Direct Med CA	C61029C8EEE3CE08755D562BB50C5F75E0EF849214970B13BD99185367D1D119	6/3/2014	6/3/2024
DigiCert Secure Auth CA	24E9F20AC167BB8F09DE8A1E9968CC53F0B5F3A4948F51B8647B40B186C75EBE	4/23/2014	4/23/2029
DigiCert Secure Server CA	94D4ECE2ED9A5457B969A13B260489E9A5FE4790A041F27A3EB4126C84418EF9	3/8/2013	3/8/2023
DigiCert SHA2 Assured ID CA	A542BCA09C5E4579C619774AE59082BCE0F86D261C5A7A5A0F6217C10279EA7C	11/5/2013	11/5/2028
DigiCert SHA2 Extended Validation Server CA <sup>1</sup>	403E062A2653059113285BAF80A0D4AE422C848C9F78FAD01FC94BC5B87FEF1A	10/22/2013	10/22/2028
DigiCert SHA2 High Assurance Server CA	19400BE5B7A31FB733917700789D2F0A2471C0C9D506C0E504C06C16D7CB17C0	10/22/2013	10/22/2028
DigiCert SHA-2 RADIUS CA	524CF7331C4EE353EEB1ECD74E1F801A0F1F08DFA0322092F42205AFC3A17675	9/20/2016	9/20/2026
DigiCert SHA2 Secure Server CA	154C433C491929C5EF686E838E323664A00E6A0D822CCC958FB4DAB03E49A08F	3/8/2013	3/8/2023

<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.



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Trusted Server CA G4	6E8D952FDBABAD8DE3D61E094393739B5A47371A52BDCB2A3C2F8C43622F640F	8/1/2013	8/1/2028
Florida HIE Exchange CA G2	AB8EE98A4B2B97E5905ECE80A64304C143AB38D9508FF7286F68235E0DB68A27	11/11/2015	11/11/2020
Google CA1	438F473EBFC8884EF5D3E0D52D264CDBE56CA382D9EBFC689D77489409F55A6E	8/25/2015	8/25/2025
Greenville Health System CA	06433FCA9F753980B526236DD72846EC1B20770BFCC7D3188DD67BC0ECFB7782	3/5/2014	3/5/2024
Highmark Tapestry HIE CA	1B68286DEFCE036512A5DAC76C8ABD067D33A07D4E0DEF7707089C980075E192	8/19/2014	8/19/2024
Huntsville Hospital System CA	20E3E88747A8D88E11A527521032DC8CAE92BC33B45C93EEE04F624A70DC920A	3/5/2014	3/5/2024
Indian Health Service-RPMS DIRECT Messaging CA	C07E9037CB81012D3046613285C14B63A0284964A4F5A821FC3B18ECDEBA0A66	4/4/2014	4/4/2024
Inland Empire Health Information Exchange	1E72D83ED9499CBA686968452BE591C48816EC9181391A5D03C1F4D3BA1658DC	1/8/2014	1/8/2024
Inpriva Direct Federated CA	5AE4F777426BBC5AA85986CA48D319270C5536210DC8EA1A28D502F6B3595138	11/18/2011	11/18/2021
INTEGRIS Direct Intermediate CA	97D276C5FDF2DC94539ABB9E17BC3995730CD51739EAE95B0F67B39E99905F11	11/18/2014	11/18/2024
iShare Medical Direct Intermediate CA	4C0A5888C34AA01B745F4EBA268696B2CCB3F4AA31C8EDCB3AFE8FA84CB74CC1	1/14/2015	1/14/2025
Jax HR Saint Vincents HIE CA	3D2928A2988227CE4EBC319AA34E6552E9D98839D5CE2114E79F8F5EC2BF9DE0	2/16/2015	2/16/2025
KeystoneHIE KeyHIE CA	D1C2009D472835AFBA94CC8ACB06DD0C727138AE1E73834394D27B0C06CF1265	8/19/2014	8/19/2024
Louisiana Health Care Quality Forum CA	3E4F09D65438B5CF7E456288C08FE9F47ED4E3ED669279C81AEFAB0BAFB86A09	10/22/2013	10/22/2023
Mary Washington Healthcare CA	1180C33AE1F23228923F6AE698C9C10DC729E0D811FC8B2EC02726E2DC26E2E4	3/5/2014	3/5/2024
Mass Hlway CA	23BA3A97C580DF2C316624D7FA5F7663580261CB2048142C73A3E86B113EB26D	9/25/2015	9/25/2025
MedicaSoft Direct Intermediate CA	51A6E2ED4104AAE8E089FBABFE26A38D656F5B0855635352FEE9598286BB021	4/28/2015	4/28/2025
Medicity Direct CA	231BA402E28B3495F3BE0CAD87078D9B8FBD86041116AF9B8047E7B1CFFA82D0	2/13/2014	2/13/2024
MHIN Direct CA	EAEFEB08D568E7F6CF6D892CAB6A22E14F20C6F10E3A418CFB42B1230933367	1/8/2014	1/8/2024
Mirth Direct Intermediate CA	CC9FAAD83C3350943D4E45FA416C4F8BC564F7AA94CF4B2D2BCE74209D0464C9	9/26/2014	9/26/2024
Mississippi Division of Medicaid CA	1757291A3D7D0BB5B9B9CF8802F1B2AE173E56B0935970FC86B63A27499DB5E2	1/8/2014	1/8/2024
MobileMD Direct Intermediate CA	33CF1F5C9396D7EE9E8283B2E76F400E50450575EB15AD02C956C1C5575B184D	10/21/2014	10/21/2024
MRO Direct Intermediate CA	E25DE970AA8B685CDF55417897F65DE64C63A55D61EE9E4B830261DCFBFFFB4	10/21/2014	10/21/2024



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
NCC Group Secure Server CA G2	6075DA5CECD15D6584C5560322D5C09FC2199E52DEA7921D91040AA75248672E	7/30/2014	7/30/2029
NCC Group Secure Server CA G3	963056B0D941D9DBE27AC778053D85E43CC79F476AD34CFDD799C27E381840EB	7/30/2014	7/30/2029
NCC Group Secure Server CA G4	B7DFDC27E5FF9F35EFEC9F4BC532C35F727789B69C90A0489B40247299D97038	7/30/2014	7/30/2029
New Hampshire Health Information Organization CA	37E9A271EB4725C93CDAF183562C7D7D9EA8FC139F8374FFE418D77D32428FE0	10/22/2013	10/22/2023
New Mexico Health Information Collaborative CA	10BEDDC480AA27563480B1BCAAB6C25B52995EA836E9A2ACE83F8F59206E2496	9/26/2014	9/26/2024
North Carolina Health Information Exchange CA	C4A842434ADB52809526B6D1E869A265F535B69BB16454A301667CC942678D58	3/5/2014	3/5/2024
North Dakota Information Technology Department CA	6ECF658CCEA8B29BE60C85904F4ADD7CCB7950CF58C97BBF60D57CEA49A2703D	1/10/2014	1/10/2024
Oklahoma State Department of Health CA	77ABE65DF4BE94E5EC222FC905E1233F8C77D6B3AE2933346A0C2FC3B2F1F560	2/16/2015	2/16/2025
Optioncare CA	89CFBC8FBFF7FE026B6CF2EA688419BDE8BBC1FB451329C865D6C6CBCF6BD097	3/1/2016	3/1/2026
Optum Public Trust CA 1	253E3C9732DF8874C3D54DA522C1711142C98C2CEA7664635152A89A03EE9364	4/28/2015	4/28/2025
Oregon Health Authority Direct CA	86FFEA40F36FA6913278710FEABA9B206F3288DA3FD1C652BC5B5895A2B1A877	3/5/2014	3/5/2024
Orion Health Direct Secure Messaging CA	A4106DA85F7B34A6D3DE37884D1528916B84F046FFB7D4AAC521117B0C6995F3	10/21/2013	10/23/2023
Orion Health Direct Secure Messaging Public HISP CA	D34138ED1458AE7DE4EDEA36ED3992E4F46E6EC9CF1E633E538DE9FF0F38F8E5	10/22/2013	10/22/2023
Plex Devices High Assurance CA	48A7C9C5A36734FC9E204D63CE6BBBCD9E21C1978604760CD8D30D6F4C67B67C	1/14/2015	1/14/2025
Plex Devices High Assurance CA2	50D3D71FC0CD7E36ADAE32221FEFBE8CC29B2676BA326C09B8FA1B24DBE75514	5/19/2015	5/19/2025
Postecom CS4	C1685683F3C8590E88580197F219CAB99E5482A1568635F596D09867B2F405BD	4/26/2016	4/26/2023
RelayHealth Direct CA	77537682E9A0B2C5BD5E62BC1CB35ECEB38FCBEBF7D2DC326F7E420F0DDBEDB3	4/4/2014	4/4/2024
Rochester RHIO Intermediate CA	43202B9E870659921F9DA26EDA9E47BF6990DB031A0BC0B23AFA1E7968ED3E99	10/21/2014	10/21/2024
Rush Health CA	DB12B1D3F8CC52FFF4874F0A8B85E9FB6A2050861B1B1C61481A743AC0D33D5A	4/23/2014	4/23/2024
SCHIE Direct CA	443C8158264710C0B768A8170E59BF1FAE4079D2BC39939A79FA839174ED81AE	6/7/2016	6/7/2026
Secure Site CA	D3533B732A518A6DA68EF266085E11DFD114C0EB0092CD43530A44D54B913ED1	2/9/2018	2/9/2030
SecurityMetrics DigiCert CA	F32DEAF22CE724661F53D5287311AFF2541EB38ECAFA9DD877B94023E3A11B1F	10/30/2012	10/30/2022
SecurityMetrics DigiCert EV CA	6B2328E7FFF598B2ADF90B7F3EA42B45FA06D78E2B117B7D60E99E828CF7565	10/30/2012	10/30/2022



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Sonavation IoT CA	4C56CA7A3C10EB58765E0FFCF8035C57C9F3BDB014862F676756CF789193F10E	5/19/2015	5/19/2025
Sutter Health CA	603D69822381A0BFC274BBED67009BC7DF133CB902FA242CF58BF727D23D5495	10/21/2014	10/21/2024
TERENA eScience Personal CA 3	FDA947208BFA3203A6C57B8714A647B7009E5168E88951345450B1D2D3F91A7D	11/18/2014	11/18/2024
TERENA eScience SSL CA 3	E1BE6BBBB70F5A241E736FC44CA2160BF6CE19B95EDD67BF7BE896E83778745	11/18/2014	11/18/2024
TERENA Personal CA 3	DD4E0C17900F3FC2A5B7B773AE40218AD73216B5CE5D285EBFFCE8830D0F034A	11/18/2014	11/18/2024
TERENA Personal CA 3 G3	C123F5AFACC9F9096809850355E5BF78CA9377348111B5167A964DDEDCC044DE9	12/9/2014	12/9/2024
TERENA SSL CA 3	BEB8EFE9B1A73C841B375A90E5FFF8048848E3A2AF66F6C4DD7B938D6FE8C5D8	11/18/2014	11/18/2024
TERENA SSL CA 3 G3	C9D6913F3FEDDEFF184C9EE1D7E17C5AEC90886EED5CC3D6E98105831C8C0E0B	12/9/2014	12/9/2024
TERENA SSL High Assurance CA 3	BE6A0D9E1D115F2293F6ABF11B3EC8E882E24426EEEB09AAA503597993E77A25	11/18/2014	11/18/2024
The Koble Group CA	A576C29481F5A2ACB1DF47500629A60F96F6ACA324E878FFDCFABD85E5649AEF	6/21/2016	6/21/2026
Trust Technologies Global CA	191E0B48B78B7EFA4822A465AD69B34405B878D10BD853D8E57C8B89D9E50B8B	8/24/2017	5/10/2025
Western Connecticut Health Network CA	415322F3970C8CD0F54311E0F93C5F5C37BA3059FDB10F5240AC20934717F840	3/5/2014	3/5/2024
WoSign EV SSL Pro CA	891EE2E23282E5076C9AE9047DE8EA900E066F81D6DC9B843C59078B0F105BC	5/23/2017	5/23/2027
WoSign OV SSL Pro CA	AA61C2927DC89DB225CA9A17D600373D058F696D86D10E2BD7B5E8F44A97EED1	5/23/2017	5/23/2027
WoTrus EV SSL Pro CA	070531383CCD100D3E9CD964DB07AA5E845A0686F2EAE3BC8A627B182057B1F1	2/9/2018	2/9/2028
WoTrus OV SSL Pro CA	09033FE23996FE4A59C4C0F523D2560E31DFE4C17D8EA1403D429A971F4BD65A	2/9/2018	2/9/2028
DigiCert EV Code Signing CA (SHA2) G1	8A78B966C73D769040C1A81C32168CEF8B9B9E96ECC2D33CC4ABB5A0CF8C1C67	4/27/2018	4/27/2028
DigiCert SHA2 Assured ID Code Signing	4ADB819C250A2E183313405499D8735299C88F970A5019A27566B27E5818F41B	4/27/2018	4/27/2028
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
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



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Secure Site Pro CA	BA6A0C1170E1C7323860749B5E7B0ED365975D8FC90740B15D70F843A2394942	4/27/2018	4/27/2028
Secure Site Pro ECC CA	A206644F57AFD10B94169498858981C16D633858CE0C88B57CF14FA2A92AACFD	4/27/2018	4/27/2028
TrustAsia ECC OV TLS Pro CA	F1CACA6AB2350A7668C13E41960908681DAFCC7E368DCB8D47FECF9631390481	4/27/2018	4/27/2028
TrustAsia OV TLS Pro CA	33E8A4ED48930760CE1AD7A2D44F079B22F660052753976109E6FC74752552BD	4/27/2018	4/27/2028
TrustAsia Secure Email CA	047217772051D292238F3355F5C5435E9B84364CCD143FC49F9C31CD605439F0	4/27/2018	4/27/2028
TrustAsia Secure Enterprise Email CA	3D774B65EE95FD6EFD1C8732B57E607C9BEE423C36E46F6E1CC8CA1F0AE62E23	4/27/2018	4/27/2028
Secure Site CA	B26EB310F8FAFOEF5B0D0B71AA65EC050FA3ADE29134FB438AB6440288FA6E67	5/17/2018	5/17/2030
TrustCubes ICA G1	2106CC7907C64B8A5DA2FC338EE94DFFF10EF711DEDDB4FC694EE092EC532B1D	7/18/2018	7/18/2028
GeoTrust Code Signing CA - G2	8D7C499D7FE9EEEC05D9EB42F03EFE402807919803E8E6CD6C1F2BF5EF6A7D8F	7/18/2018	7/18/2028
DigiCert SHA1 Assured ID Code Signing CA - G1	82AD46ECDE882413106B1C83EF65DC02DB0C65B3870F6F744B62283DF6FA1D56	7/18/2018	7/18/2028
DigiCert SHA2 Assured ID Code Signing CA - G3	9CDFD82596D1BAC9E44D3E491E2C07D8DCC920419915FD6F361CF70A1E433B10	7/18/2018	7/18/2028
GeoTrust Code Signing CA	78A95ED82180A1C33A9F34EDB75E6774FD4BB73AA2C7C4121453DDB627DB1BAF	7/18/2018	7/18/2028
DigiCert SHA2 Assured ID Code Signing CA - G2	2A9D0D018BB49FDEA14D6C16E9BA0A942F2833B9AADFFBAD1306E301B495CFB7	7/18/2018	7/18/2028
DigiCert EV Code Signing CA (SHA2) G2	EDCD88B6BD77FC8A2680E2ECB8FFBAC45898DFA0FDE983425E0F1BEB058C04B6	7/18/2018	7/18/2028
DigiCert EV Code Signing CA (SHA2) G3	2B0A972DC0DAE218E9477396D3D82DEB82DE118867DD19E1D2FFFD958CBB6DA9	7/18/2018	7/18/2028
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 Japan CA	AD14A68BEC949E84F6063419D63465D137C2ADD3E3A85E00E9E3EE82E5B4018F	11/20/2018	11/20/2028
DigiCert Secure Site Korea CA	6555D661D37F249A23C2D5F83479E78051B6DE76A147B506D6BEA2882B4D066	11/20/2018	11/20/2028
Thawte Partner CA	635AF6889F49060FE0E7BABC0F23314FB118F3B18243DD17F47D8647A69684B1	11/20/2018	11/20/2028
Riverbed Certificate Issuer	BB39497035ED9583D286CDE70FB644EB95806598092B1E8D8F11BC035D7A476A	11/20/2018	11/20/2028
RVBD Certificate Issuer	72563CC98ADA2C5D2126542ACC908154AEB1F9D6F7E83A55C09744C7D7ADDDBA	11/20/2018	11/20/2028
SGN FISGLOBAL PUBLIC CA	0AD6A7334A5A23C986980F6FECD25006B563A0B6F1BCAA65C0345BA2D96928D3	1/8/2019	1/8/2024



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
WIPO CA - G4	16D809ED155C2AC7E9489E1A204116C9D16EFBE4C91F53369725A2B395535E28	1/29/2019	1/29/2024
DigiCert Secure Site ECC CA-1	99935E20424535EC016F337B2BE68F1349DE66CCE4CA5AB367F8F3738215B833	2/15/2019	2/15/2029
DigiCert Secure Site Korea ECC CA	EF9138993654DF92D2FB5860E28DE8818A9F49DB56ECB689A67A7FC2D5881DD2	3/25/2019	3/25/2029
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
DigiCert Class 3 ECC CA G1	CBAE2767EE8CD7FB49B662B422F721DB4522EB674CDBF16CB6209E45CC4CB99E	11/2/2017	11/2/2027
DigiCert Class 3 RSA CA G1	81E071B01F01DC43EE458C0E1BDCBC848B47462C26B4CE19EE9015416BC6DF89	11/2/2017	11/2/2027
TrustAsia ECC CA G9	45B2A3A4D06EE652E940FABCA5CD8721C1FB7FEED8B75B0CC7F067E1D26E2CFE	11/2/2017	11/2/2027
TrustAsia RSA CA G8	48C4A1C5395E2B499D2E3EBE26EEFA91D11CF35DD5FA14937EEE5E807A2FF487	11/2/2017	11/2/2027
TrustAsia TLS ECC CA G9	877F24CE70F4A3047E4EA70BEC1BC31BE9B6533ADFF3A393FF9BFB3C81029446	11/2/2017	11/2/2027
TrustAsia TLS RSA CA	79F1F5AB697DEBF195F5B7DA65F95399682EDAEB80115B9D42A6AE5E2FA98802	12/8/2017	12/8/2027
TrustAsia TLS RSA CA G8	036A18F5F0EB9DD5EE02B7854DF5C33845601D8939CFB7B607F69D142C01D909	11/2/2017	11/2/2027
Amazon	ECC295B6DDC084BA7179FB53BDD1D422CB6C0A8D94F154D4A5B17780B7279ED	7/16/2018	7/16/2028
TrustAsia TLS ECC CA	68D0B2E8C85BF009B4DB39AC8B5E2FA8E1FD9FD1E5028704EA9288C7E472AAEB	12/8/2017	12/8/2027
DigiCert High Assurance Code Signing CA-1	BEAF46D0FF62645F56BE11830DDEF663379619F337E85713491C83AE179481D	2/10/2011	2/10/2026
DigiCert Assured ID Code Signing CA-1	E57208CBFD286CE9718267E44491CB5B435C95BB09DC9720F5B64B25AC7974CD	2/10/2011	2/10/2026
WFA Hotspot 2.0 Intermediate CA	FEA342D00D1A355CF51569EF7E0F617ABB0F22D6D1E73DAA11DCB4D407975543	11/25/2013	11/25/2023
DigiCert CN RSA EV CA G1	B131905CC7221270613B529AC9E786AA230ABFE154A0ACBE452BC350BD1EFE4B	6/20/2019	6/20/2029
DigiCert CN RSA CA G1	03CE9BC71B91FDB7CB3C5235CAE0701CB486BBD628D4AADE5841FC5F0AA37A46	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
DigiCert Global CA-2 G2	1C00D61F6C7EDCB3755535D1BE1A0EC1F94A4BB24E1A7A50241A556CD74F3A0	10/16/2019	10/16/2029



## DIGICERT, INC. MANAGEMENT’S ASSERTION

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

DigiCert management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its 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 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 SSL certificates in conformity with the CA/Browser Forum Requirements on the DigiCert [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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#).

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



Mozilla Bug #	Description	Date Opened	Date Closed
<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
<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





Mozilla Bug #	Description	Date Opened	Date Closed
<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 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	802447EE521CC666CDB7BBAE93A385E55F200D76A3D1356A85445AC4CDBED12	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
Hotspot 2.0 Trust Root CA - 03	A3CC68595DFE7E86D8AD1772A8B5284ADD54ACE3B8A798DF47BCCAFB1FDB84DF	12/8/2013	12/8/2043
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



Cross-Signed Root CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Global Root CA	6DACBB8945137B1DAD4211B0436EFBE06F12ACE36904973B45AE25740823D369	12/7/2016	5/10/2025
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
AAMC Direct Intermediate CA	BB1C01E884DD0919AB94D5AF5575CD6FEB71E560B2B58735A78B150A10D54BF3	5/28/2015	5/28/2025
Abbott Laboratories Secure Authentication CA	DB99A4F284CCF10B26DE7B7A5D651725B857CBC871EBB33028D67B55510EFC9D	8/23/2016	8/23/2026
Abbott Laboratories Secure Server CA	6C69E201656440EB98CD0875764A1ED19015ED8C4427601ACA9C68AFA8973959	7/12/2016	7/12/2026
Adobe Analytics - DigiCert CA	D5C009312F845C5EC8506EAD560D62447BFF4A60A9C25210511217AD6DE76AED	4/18/2013	4/18/2021
Aetna Inc. Secure CA2	5D28761CBF304EAFCD127B34D614FE179AC7744F1552AF1C31298425AD05A275	12/9/2014	12/9/2024
Aetna Inc. Secure EV CA	0A163600631BD66267FB7AEAD25C538B2B7D72AD6416A2BBD285F654BB642F6D	12/9/2014	12/9/2024
Aetna Inc. Secure EV CA2	1DDFDDF883E3945B2CB24FA5B83788379C5AB058422AB979DF66C77473988687	12/8/2017	12/8/2027
Alaska eHealth Network CA	437859303D0183862A96F6ABF8B03F2A69D4CBD317217666015E1ABA3C84AA11	10/22/2013	10/22/2023
Allina Health Connect HIE Intermediate CA	826C6AA610EF190BE2D7C03E22D032405B289804E3319E233C4C37FFBF305F1A	12/8/2015	12/8/2025
Amazon Server CA 1B	4A1FF6BBF481170D3B773CEC1F3A84DE3B5096575CDBF8B08432209318CA0FBFD	10/21/2015	10/21/2040



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Amazon Server CA 1B	F55F9FFCB83C73453261601C7E044DB15A0F034B93C05830F28635EF889CF670	10/22/2015	10/22/2025
Axesson Direct CA	BF4655F16AA338D7C7FF2BDC949A524BD4797B8B3C8341C608C9F65CB1CB8177	1/8/2014	1/8/2024
Cal INDEX CA	A5226F33474B53392665298B48F4E6129824E98BD4D38DF4E31EBBCF14FA33CD	7/12/2016	7/12/2026
Care360 Direct Intermediate CA	2D602B1F166D6316DAFD46B4B1EDD6DCFC54D2AF8A944BE358858FD504AAA16B	8/25/2015	8/25/2025
Catholic Health Initiatives CA	151A3591B765D02C359EEC9C56ED8DDAD0C54E756A497D02BF979FA8DD5D95BB	8/19/2014	8/19/2024
Cerner Corporation Direct Intermediate CA	09DE7FA739EE47C06291845F2E0E8A9E1C7CC2900AD354CF167316E02386BD9B	9/26/2014	9/26/2024
Cerner Corporation Resonance Intermediate CA	64284AA5F8DC8697D43D9737CF4E266625414E449C019667714537FF7EDE31B7	11/11/2015	11/11/2021
Cisco Meraki CA	199EE58009555DAE2CDA0626931C64391D6A88CCCB1F9F0B2EE80B667F581C06	7/12/2016	7/12/2026
CloudFlare Inc ECC CA-2	6172D7A1996CBEF71A0182DD44B99E9C035742A9EBD0311AA73AA4733344C5A6	10/14/2015	10/9/2020
CloudFlare Inc RSA CA-1	328C5991D8383E27D0EBE910BF66C0AF3D748A85D3011A52D88F1D8C8635647F	10/14/2015	10/14/2020
CompuGroup Medical Certificate Authority	B604026A3590392ABEFB6B18E8176453656115D2A0060F713E191A9FD076532A	12/8/2015	12/8/2025
Corepoint Direct Intermediate CA	CD2640957CF88610470CEFD409D85D9BE05962F7D6C2999C4F431ABCCC34118C	1/14/2015	1/14/2025
Cybertrust Japan ECC EV CA	92E3770B1EB44F84C2F2CB0097C2FD7126BD212B41C2610E78DDFD8946761738	8/24/2017	8/24/2032
Cybertrust Japan Extended Validation Server CA	0E10BDDEE7512DBD79EBF0B4F48FEED7C83C2BD3DD81765565F4FF110B7BFA42	12/7/2016	12/7/2031
Cybertrust Japan Issuing CA-1	87942388D29A46C06FE1E56AAB791594D0FB2E8EABF124048F130EEA9BEDD3FD	9/1/2016	9/1/2026
Cybertrust Japan Secure Server CA	33D57359831F87754E6E755D6B5B56E7E71297DDDFEA1D6397086604280F6FFC	12/7/2016	12/7/2031
Cybertrust Japan Secure Server ECC CA	C3683F7D91754219DADA4E8DC30E4B18BD3928B53D3AB93D07384BC5871CE355	7/13/2017	7/13/2032
Data Management Intermediate Certificate Authority	54837EF7B5AC4AA23606A15EF30DE46E9BB7E23E60F6ED4F2612092B94EDC68F	8/25/2015	8/25/2025
DC Government SHA2 Assured ID Intermediate CA	FB1147E7AB97A29BB9C1140ABF3DE831F4C5F60D11B90FEC999A0816375D8457	7/13/2017	7/13/2027
DC Government SHA2 EV Intermediate CA	F12241EE34C03A608D34DBC0EA465E1BD1AA13091554F9D4D086253FF3CE83D4	7/13/2017	7/13/2027
DigiCert Accredited Direct Med CA	0E78434EC8AD6613562C8390D8B3306FC6087E0593C7D5AC2FAF9AD263879745	8/6/2013	8/6/2023
DigiCert Assured ID CA G2	93C381CB07B353A920C2A7BED6BEBF195C68279DD0527D37F20BDD0D99C330FA	8/1/2013	8/1/2028



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Assured ID CA G3	634FDF26C994E76A2918D9EFC4CAB9C6FCB344EF642A79C89192BCDA0ED52F4C	8/1/2013	8/1/2028
DigiCert Assured ID CA-1	425E72C87FF22855D9908B71AB4C64B0D2F248287097690C62FE733F631DE38F	11/10/2006	11/10/2021
DigiCert Assured ID CA-1	B8F44E4B1F8697DF54BB3D0F1E67596CE2FE9DABA85AF4E6F2A2E74396F8C56D	11/10/2006	11/10/2021
DigiCert Assured ID Intermediate CA (SHA2)	C2B4BBEF4A1A643F334ED0850F928876D2AE3AE3642B986014D68C673C04D081	12/7/2011	12/7/2026
DigiCert Assured ID TLS CA	D7737E5F2D3FFCA429902E9F388CFD6C5959CD35A0FC103CEE2F7E93D1C66A52	2/9/2018	2/9/2030
DigiCert Baltimore CA-1 G2	BF1CB0E213D8D3C70BAE89429FC16DE2C74F755963D1B9B488BD0260DBC91B9C	10/14/2015	5/10/2025
DigiCert Baltimore CA-2 G2	F9690880819F06CDCC0B2F224B207F2AF6003FB57339B8679A160FA95208D62D	12/8/2015	5/10/2025
DigiCert Baltimore EV CA	D46931E0182DD655EA0C16E6DD99F8E61AFFE401F734C6CA8EA0056A968EAF81	10/14/2015	5/10/2025
DigiCert Cloud Services CA-1	2F6889961A7CA7067E8BA103C2CF9B9A924F8CA293F11178E23A1978D2F133D3	8/4/2015	8/4/2030
DigiCert Direct Non-Provider CA	1AEDDADDC1ED748543EAF5960DF96AD51E21A3164F30A0640CB0732365D39062	2/11/2014	2/11/2024
DigiCert ECC Extended Validation Server CA	FDC8986CFAC4F35F1ACD517E0F61B879882AE076E2BA80B77BD3F0FE5CECF8862	6/21/2016	6/21/2031
DigiCert ECC Secure Server CA	458446BA75D932E914F23C2B57B7D192EDDBC2181D958E1181AD5251747A1EE8	3/8/2013	3/8/2023
DigiCert EV Server CA G4	710024B37BD9F0E1537C18A4C20F9A31C4B485D1248C643F20B4C00F3716BA85	1/17/2017	1/17/2032
DigiCert Extended Validation CA G3	7C0912E5DE8478BB86E8EA46BA5AE65DC3870BCEFCBC2F46795EEECF648CFBE7	11/11/2015	11/11/2030
DigiCert Extended Validation Intermediate CA (SHA2)	802C2AD1D215E57CDC9010EA437ACE399B657194FBD40E3BB5E00B080E6496DF	12/7/2011	12/7/2026
DigiCert Federated Healthcare CA	54C3F501042CDCC09AE8143CB192BD5E5724C9C88A6AB395A94A1A7AFC26CE7C	2/11/2014	2/11/2024
DigiCert Federated ID L1 CA	CAB016C5EA32061BD065FE13A55A40FA61058B27B34A7F8D175F7101EE063E3B	10/30/2012	10/30/2022
DigiCert Federated ID L2 CA	91FDEB52D4265120B843B195D1B6CDB5CE61251865A45A3E920E610FDDA660D3	1/7/2014	1/7/2023
DigiCert Federated ID L3 CA	85760F77DB0FD0D93C21EE0364B8EAB09B82CF49B7849831038209B5B1081363	1/7/2014	1/7/2023
DigiCert Federated ID L4 CA	EFB2A3F37273D3589047919825EA5337E9B938A8C178B61C18C2B4270B9665AC	10/30/2012	10/30/2022
DigiCert Federated ID US L3 CA	EB84FC0B403D9B689297A5D83EA186838E3B777BC618EFDA162A75B7FEA666C1	1/8/2014	1/8/2023
DigiCert Federated ID US L4 CA	6797436214EFEE67CDE7D70358D4D8B00DFBF78D5C87C62B4A7E790D73DD7BD9	4/18/2013	4/18/2023



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert Federated Trust CA	E5BBDDCAD572EC9D2DD96E0E5EBF049A9181F070F1E33CC1635AD8EC487D2177	11/18/2011	11/18/2023
DigiCert Global CA G2	8FAC576439C9FD3EF153B51F9EDD0D381B5DF7B87559CEBECA04297DD44A639B	8/1/2013	8/1/2028
DigiCert Global CA G3	F7541CF69D1DE1AC953ABC1FAD6F7807A34EDFE9E12C11E66A195930C23AD6C6	8/1/2013	8/1/2028
DigiCert Global CA-1	3C750409882486D64151F4CBB5BD61432A4A7BF42F48A85198D245A64AEA2117	11/10/2006	11/10/2021
DigiCert Governmental Direct CA	5F665CBACC1E37171EA83EA85C570F9861CAF77BAC8886ABC4BB19B3698C094A	9/25/2015	9/25/2025
DigiCert Grid Trust CA	1E0A3AB993157717281D42ABF801EB64DEED500E4168CA706D6A71D8103C73A2	12/7/2011	12/7/2026
DigiCert Grid Trust CA G2	28CBB4E0D9C4EE6D04AC8F14717605AE3A4BD8CBF8D081B27AF6EDB2F3D76A32	1/8/2014	1/8/2029
DigiCert High Assurance CA-3	21EB37AB4CF6EF8965EC1766409CA76B8B2E03F2D1A388DF734208E86DEEE679	4/2/2008	4/3/2022
DigiCert High Assurance CA-3	57D8D5B832616B7823466A0C372770D16A5DCF246581F0F58373E51C7E1E5316	4/3/2007	4/3/2022
DigiCert High Assurance CA-3	COA4A1AC05E03096A3B2AB8A38502B39E2614E11397BEE73D0A66B8ACEF7A283	4/3/2008	4/3/2022
DigiCert High Assurance CA-3	DCB400ACC249FB8483415FC2650BC90488CA96643118CB0E4F4424B21C3AA5A4	10/12/2011	4/3/2022
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
DigiCert High Assurance Intermediate CA (SHA2)	47511629F2BC3B7CF84EFEC9F32798A43AF6252E550B6CAE76A38558712E37D8	12/7/2011	12/7/2026
DigiCert Provisional Direct Med CA	C61029C8EEE3CE08755D562BB50C5F75E0EF849214970B13BD99185367D1D119	6/3/2014	6/3/2024
DigiCert Secure Auth CA	24E9F20AC167BB8F09DE8A1E9968CC53F0B5F3A4948F51B8647B40B186C75EBE	4/23/2014	4/23/2029
DigiCert Secure Server CA	94D4ECE2ED9A5457B969A13B260489E9A5FE4790A041F27A3EB4126C84418EF9	3/8/2013	3/8/2023
DigiCert SHA2 Assured ID CA	A542BCA09C5E4579C619774AE59082BCE0F86D261C5A7A5A0F6217C10279EA7C	11/5/2013	11/5/2028



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
DigiCert SHA2 High Assurance Server CA	19400BE5B7A31FB733917700789D2F0A2471C0C9D506C0E504C06C16D7CB17C0	10/22/2013	10/22/2028
DigiCert SHA-2 RADIUS CA	524CF7331C4EE353EEB1ECD74E1F801A0F1F08DFA0322092F42205AFC3A17675	9/20/2016	9/20/2026
DigiCert SHA2 Secure Server CA	154C433C491929C5EF686E838E323664A00E6A0D822CCC958FB4DAB03E49A08F	3/8/2013	3/8/2023
DigiCert Trusted Server CA G4	6E8D952FDBABAD8DE3D61E094393739B5A47371A52BDCB2A3C2F8C43622F640F	8/1/2013	8/1/2028
Florida HIE Exchange CA G2	AB8EE98A4B2B97E5905ECE80A64304C143AB38D9508FF7286F68235E0DB68A27	11/11/2015	11/11/2020
Google CA1	438F473EBFC8884EF5D3E0D52D264CDBE56CA382D9EBFC689D77489409F55A6E	8/25/2015	8/25/2025
Greenville Health System CA	06433FCA9F753980B526236DD72846EC1B20770BFCC7D3188DD67BC0ECFB7782	3/5/2014	3/5/2024
Highmark Tapestry HIE CA	1B68286DEFCE036512A5DAC76C8ABD067D33A07D4E0DEF7707089C980075E192	8/19/2014	8/19/2024
Huntsville Hospital System CA	20E3E88747A8D88E11A527521032DC8CAE92BC33B45C93EEE04F624A70DC920A	3/5/2014	3/5/2024
Indian Health Service-RPMS DIRECT Messaging CA	C07E9037CB81012D3046613285C14B63A0284964A4F5A821FC3B18ECDEBA0A66	4/4/2014	4/4/2024
Inland Empire Health Information Exchange	1E72D83ED9499CBA686968452BE591C48816EC9181391A5D03C1F4D3BA1658DC	1/8/2014	1/8/2024
Inpriva Direct Federated CA	5AE4F777426BBC5AA85986CA48D319270C5536210DC8EA1A28D502F6B3595138	11/18/2011	11/18/2021
INTEGRIS Direct Intermediate CA	97D276C5FDF2DC94539ABB9E17BC3995730CD51739EAE95B0F67B39E99905F11	11/18/2014	11/18/2024
iShare Medical Direct Intermediate CA	4C0A5888C34AA01B745F4EBA268696B2CCB3F4AA31C8EDCB3AFE8FA84CB74CC1	1/14/2015	1/14/2025
Jax HR Saint Vincents HIE CA	3D2928A2988227CE4EBC319AA34E6552E9D98839D5CE2114E79F8F5EC2BF9DE0	2/16/2015	2/16/2025
KeystoneHIE KeyHIE CA	D1C2009D472835AFBA94CC8ACB06DD0C727138AE1E73834394D27B0C06CF1265	8/19/2014	8/19/2024
Louisiana Health Care Quality Forum CA	3E4F09D65438B5CF7E456288C08FE9F47ED4E3ED669279C81AEFAB0BAFB86A09	10/22/2013	10/22/2023
Mary Washington Healthcare CA	1180C33AE1F23228923F6AE698C9C10DC729E0D811FC8B2EC02726E2DC26E2E4	3/5/2014	3/5/2024
Mass Hlway CA	23BA3A97C580DF2C316624D7FA5F7663580261CB2048142C73A3E86B113EB26D	9/25/2015	9/25/2025

<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.





Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
MedicaSoft Direct Intermediate CA	51A6E2ED41040AAE8E089FBABFE26A38D656F5B0855635352FEE9598286BB021	4/28/2015	4/28/2025
Medicity Direct CA	231BA402E28B3495F3BE0CAD87078D9B8FBD86041116AF9B8047E7B1CFFA82D0	2/13/2014	2/13/2024
MHIN Direct CA	EAEF808D568E7F6CF6D892CAB6A22E14F20C6F10E3A418CFB42B1230933367	1/8/2014	1/8/2024
Mirth Direct Intermediate CA	CC9FAAD83C3350943D4E45FA416C4F8BC564F7AA94CF4B2D2BCE74209D00464C9	9/26/2014	9/26/2024
Mississippi Division of Medicaid CA	1757291A3D7D0BB5B9B9CF8802F1B2AE173E56B0935970FC86B63A27499DB5E2	1/8/2014	1/8/2024
MobileMD Direct Intermediate CA	33CF1F5C9396D7EE9E8283B2E76F400E50450575EB15AD02C956C1C5575B184D	10/21/2014	10/21/2024
MRO Direct Intermediate CA	E25DE970AA8B85CDF55417897F65DE64C63A55D61EE9E4B830261DCFBFFFB4	10/21/2014	10/21/2024
NCC Group Secure Server CA G2	6075DA5CECD15D6584C5560322D5C09FC2199E52DEA7921D91040AA75248672E	7/30/2014	7/30/2029
NCC Group Secure Server CA G3	963056B0D941D9DBE27AC778053D85E43CC79F476AD34CFDD799C27E381840EB	7/30/2014	7/30/2029
NCC Group Secure Server CA G4	B7DFDC27E5FF9F35EFEC9F4BC532C35F727789B69C90A0489B40247299D97038	7/30/2014	7/30/2029
New Hampshire Health Information Organization CA	37E9A271EB4725C93CDAF183562C7D7D9EA8FC139F8374FFE418D77D32428FE0	10/22/2013	10/22/2023
New Mexico Health Information Collaborative CA	10BEDDC480AA27563480B1BCAAB6C25B52995EA836E9A2ACE83F8F59206E2496	9/26/2014	9/26/2024
North Carolina Health Information Exchange CA	C4A842434ADB52809526B6D1E869A265F535B69BB16454A301667CC942678D58	3/5/2014	3/5/2024
North Dakota Information Technology Department CA	6ECF658CCEA8B29BE60C85904F4ADD7CCB7950CF58C97BBF60D57CEA49A2703D	1/10/2014	1/10/2024
Oklahoma State Department of Health CA	77ABE65DF4BE94E5EC222FC905E1233F8C77D6B3AE2933346A0C2FC3B2F1F560	2/16/2015	2/16/2025
Optioncare CA	89CFBC8FBFF7FE026B6CF2EA688419BDE8BBC1FB451329C865D6C6CBCF6BD097	3/1/2016	3/1/2026
Optum Public Trust CA 1	253E3C9732DF8874C3D54DA522C1711142C98C2CEA7664635152A89A03EE9364	4/28/2015	4/28/2025
Oregon Health Authority Direct CA	86FFEA40F36FA6913278710FEABA9B206F3288DA3FD1C652BC5B5895A2B1A877	3/5/2014	3/5/2024
Orion Health Direct Secure Messaging CA	A4106DA85F7B34A6D3DE37884D1528916B84F046FFB7D4AAC521117B0C6995F3	10/21/2013	10/23/2023
Orion Health Direct Secure Messaging Public HISP CA	D34138ED1458AE7DE4EDEA36ED3992E4F46E6EC9CF1E633E538DE9FF0F38F8E5	10/22/2013	10/22/2023
Plex Devices High Assurance CA	48A7C9C5A36734FC9E204D63CE6BBBCD9E21C1978604760CD8D30D6F4C67B67C	1/14/2015	1/14/2025
Plex Devices High Assurance CA2	50D3D71FC0CD7E36ADAE32221FEFB8CC29B2676BA326C09B8FA1B24DBE75514	5/19/2015	5/19/2025



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Postecom CS4	C1685683F3C8590E88580197F219CAB99E5482A1568635F596D09867B2F405BD	4/26/2016	4/26/2023
RelayHealth Direct CA	77537682E9A0B2C5BD5E62BC1CB35ECEB38FCBEBF7D2DC326F7E420F0DDBEDB3	4/4/2014	4/4/2024
Rochester RHIO Intermediate CA	43202B9E870659921F9DA26EDA9E47BF6990DB031A0BC0B23AFA1E7968ED3E99	10/21/2014	10/21/2024
Rush Health CA	DB12B1D3F8CC52FFF4874F0A8B85E9FB6A2050861B1B1C61481A743AC0D33D5A	4/23/2014	4/23/2024
SCHIEX Direct CA	443C8158264710C0B768A8170E59BF1FAE4079D2BC39939A79FA839174ED81AE	6/7/2016	6/7/2026
Secure Site CA	D3533B732A518A6DA68EF266085E11DFD114C0EB0092CD43530A44D54B913ED1	2/9/2018	2/9/2030
SecurityMetrics DigiCert CA	F32DEAF22CE724661F53D5287311AFF2541EB38ECAFA9DD877B94023E3A11B1F	10/30/2012	10/30/2022
SecurityMetrics DigiCert EV CA	6B2328E7FFF598B2ADF90B7F3EA42B45FA606D78E2B117B7D60E99E828CF7565	10/30/2012	10/30/2022
Sonavation IoT CA	4C56CA7A3C10EB58765E0FFCF8035C57C9F3BDB014862F676756CF789193F10E	5/19/2015	5/19/2025
Sutter Health CA	603D69822381A0BF6C274BBED67009BC7DF133CB902FA242CF58BF727D23D5495	10/21/2014	10/21/2024
TERENA eScience Personal CA 3	FDA947208BFA3203A6C57B8714A647B7009E5168E88951345450B1D2D3F91A7D	11/18/2014	11/18/2024
TERENA eScience SSL CA 3	E1BE6BBBB70F5A241E736FC44C6A2160BF6CE19B95EDD67BF7BE896E83778745	11/18/2014	11/18/2024
TERENA Personal CA 3	DD4E0C17900F3FC2A5B7B773AE40218AD73216B5CE5D285EBFFCE8830D0F034A	11/18/2014	11/18/2024
TERENA Personal CA 3 G3	C123F5AFACC9F9096809850355E5BF78CA9377348111B5167A964DDEDC044DE9	12/9/2014	12/9/2024
TERENA SSL CA 3	BEB8EFE9B1A73C841B375A90E5FFF8048848E3A2AF66F6C4DD7B938D6FE8C5D8	11/18/2014	11/18/2024
TERENA SSL CA 3 G3	C9D6913F3FEDDEFF184C9EE1D7E17C5AEC90886EED5CC3D6E98105831C8C0E0B	12/9/2014	12/9/2024
TERENA SSL High Assurance CA 3	BE6A0D9E1D115F2293F6ABF11B3EC8E882E24426EEEB09AAA503597993E77A25	11/18/2014	11/18/2024
The Koble Group CA	A576C29481F5A2ACB1DF47500629A60F96F6ACA324E87FFDCFABD85E5649AEF	6/21/2016	6/21/2026
Trust Technologies Global CA	191E0B48B78B7EFA4822A465AD69B34405B878D10BD853D8E57CB8B9D9E50B8B	8/24/2017	5/10/2025
Western Connecticut Health Network CA	415322F3970C8CD0F54311E0F93C5F5C37BA3059FDB10F5240AC20934717F840	3/5/2014	3/5/2024
WoSign EV SSL Pro CA	891EE2E23282E5076C9AE9047DE8EA900E066F81D6DC9B843C59078B0F105BC	5/23/2017	5/23/2027
WoSign OV SSL Pro CA	AA61C2927DC89DB225CA9A17D600373D058F696D86D10E2BD7B5E8F44A97EED1	5/23/2017	5/23/2027



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
WoTrus EV SSL Pro CA	070531383CCD100D3E9CD964DB07AA5E845A0686F2EAE3BC8A627B182057B1F1	2/9/2018	2/9/2028
WoTrus OV SSL Pro CA	09033FE23996FE4A59C4C0F523D2560E31DFE4C17D8EA1403D429A971F4BD65A	2/9/2018	2/9/2028
DigiCert EV Code Signing CA (SHA2) G1	8A78B966C73D769040C1A81C32168CEF8B9B9E96ECC2D33CC4ABB5A0CF8C1C67	4/27/2018	4/27/2028
DigiCert SHA2 Assured ID Code Signing	4ADB819C250A2E183313405499D8735299C88F970A5019A27566B27E5818F41B	4/27/2018	4/27/2028
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
TrustAsia ECC EV TLS Pro CA	2DAAC6DFAC16C548C53FF1198254D7E937761D22A1E7CC5C1A9462E971461F5	4/27/2018	4/27/2028
TrustAsia EV TLS Pro CA	4AFFE4FEF39464D1788C660AF591D5E601B261C4811DF0A3DD9D61CAFE8E5ED8	4/27/2018	4/27/2028
Secure Site Pro CA	BA6A0C1170E1C7323860749B5E7B0ED365975D8FC90740B15D70F843A2394942	4/27/2018	4/27/2028
Secure Site Pro ECC CA	A206644F57AFD10B94169498858981C16D633858CE0C88B57CF14FA2A92AACFD	4/27/2018	4/27/2028
TrustAsia ECC OV TLS Pro CA	F1CACA6AB2350A7668C13E41960908681DAFCC7E368DCB8D47FECF9631390481	4/27/2018	4/27/2028
TrustAsia OV TLS Pro CA	33E8A4ED48930760CE1AD7A2D44F079B22F660052753976109E6FC74752552BD	4/27/2018	4/27/2028
TrustAsia Secure Email CA	047217772051D292238F3355F5C5435E9B84364CCD143FC49F9C31CD605439F0	4/27/2018	4/27/2028
TrustAsia Secure Enterprise Email CA	3D774B65EE95FD6EFD1C8732B57E607C9BEE423C36E46F6E1CC8CA1F0AE62E23	4/27/2018	4/27/2028
Secure Site CA	B26EB310F8FAF0EF5B0D0B71AA65EC050FA3ADE29134FB438AB6440288FA6E67	5/17/2018	5/17/2030
TrustCubes ICA G1	2106CC7907C64B8A5DA2FC338EE94DFFF10EF711DEDBB4FC694EE092EC532B1D	7/18/2018	7/18/2028
GeoTrust Code Signing CA - G2	8D7C499D7FE9EEEC05D9EB42F03EFE402807919803E8E6CD6C1F2BF5EF6A7D8F	7/18/2018	7/18/2028
DigiCert SHA1 Assured ID Code Signing CA - G1	82AD46ECDE882413106B1C83EF65DC02DB0C65B3870F6744B62283DF6FA1D56	7/18/2018	7/18/2028
DigiCert SHA2 Assured ID Code Signing CA - G3	9CDFD82596D1BAC9E44D3E491E2C07D8DCC920419915FD6F361CF70A1E433B10	7/18/2018	7/18/2028
GeoTrust Code Signing CA	78A95ED82180A1C33A9F34EDB75E6774FD4BB73AA2C7C4121453DDB627DB1BAF	7/18/2018	7/18/2028
DigiCert SHA2 Assured ID Code Signing CA - G2	2A9D0D018BB49FDEA14D6C16E9BA0A942F2833B9AADFFBAD1306E301B495CFB7	7/18/2018	7/18/2028



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
DigiCert EV Code Signing CA (SHA2) G2	EDCD88B6BD77FC8A2680E2ECB8FFBAC45898DFA0FDE983425E0F1BEB058C04B6	7/18/2018	7/18/2028
DigiCert EV Code Signing CA (SHA2) G3	2B0A972DC0DAE218E9477396D3D82DEB82DE118867DD19E1D2FFFD958CBB6DA9	7/18/2018	7/18/2028
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 Japan CA	AD14A68BEC949E84F6063419D63465D137C2ADD3E3A85E00E9E3EE82E5B4018F	11/20/2018	11/20/2028
DigiCert Secure Site Korea CA	6555D661D37F2494A23C2D5F83479E78051B6DE76A147B506D6BEA2882B4D066	11/20/2018	11/20/2028
Thawte Partner CA	635AF6889F49060FE0E7BABC0F23314FB118F3B18243DD17F47D8647A69684B1	11/20/2018	11/20/2028
Riverbed Certificate Issuer	BB39497035ED9583D286CDE70FB644EB95806598092B1E8D8F11BC035D7A476A	11/20/2018	11/20/2028
RVBD Certificate Issuer	72563CC98ADA2C5D2126542ACC908154AEB1F9D6F7E83A55C09744C7D7ADDDBA	11/20/2018	11/20/2028
SGN FISGLOBAL PUBLIC CA	0AD6A7334A5A23C986980F6FECD25006B563A0B6F1BCAA65C0345BA2D96928D3	1/8/2019	1/8/2024
WIPO CA - G4	16D809ED155C2AC7E9489E1A204116C9D16EFBE4C91F53369725A2B395535E28	1/29/2019	1/29/2024
DigiCert Secure Site ECC CA-1	99935E20424535EC016F337B2BE68F1349DE66CCE4CA5AB367F8F3738215B833	2/15/2019	2/15/2029
DigiCert Secure Site Korea ECC CA	EF9138993654DF92D2FB5860E28DE8818A9F49DB56ECB689A67A7FC2D5881DD2	3/25/2019	3/25/2029
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
DigiCert Class 3 ECC CA G1	CBAE2767EE8CD7FB49B662B422F721DB4522EB674CDBF16CB6209E45CC4CB99E	11/2/2017	11/2/2027
DigiCert Class 3 RSA CA G1	81E071B01F01DC43EE458C0E1BDCBC848B47462C26B4CE19EE9015416BC6DF89	11/2/2017	11/2/2027
TrustAsia ECC CA G9	45B2A3A4D06EE652E940FABCA5CD8721C1FB7FEED8B75B0CC7F067E1D26E2CFE	11/2/2017	11/2/2027
TrustAsia RSA CA G8	48C4A1C5395E2B499D2E3EBE26EEFA91D11CF35DD5FA14937EEE5E807A2FF487	11/2/2017	11/2/2027
TrustAsia TLS ECC CA G9	877F24CE70F4A3047E4EA70BEC1BC31BE9B6533ADFF3A393FF9BFB3C81029446	11/2/2017	11/2/2027
TrustAsia TLS RSA CA	79F1F5AB697DEBF195F5B7DA65F95399682EDAEB80115B9D42A6AE5E2FA98802	12/8/2017	12/8/2027
TrustAsia TLS RSA CA G8	036A18F5F0EB9DD5EE02B7854DF5C33845601D8939CFB7B607F69D142C01D909	11/2/2017	11/2/2027



Subordinate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
Amazon	ECC295B6DDCD084BA7179FB53BDD1D422CB6C0A8D94F154D4A5B17780B7279ED	7/16/2018	7/16/2028
TrustAsia TLS ECC CA	68D0B2E8C85BF009B4DB39AC8B5E2FA8E1FD9FD1E5028704EA9288C7E472AAEB	12/8/2017	12/8/2027
DigiCert High Assurance Code Signing CA-1	BEAF46D0FF62645F56BE11830DDEFC663379619F337E85713491C83AE179481D	2/10/2011	2/10/2026
DigiCert Assured ID Code Signing CA-1	E57208CBFD286CE9718267E44491CB5B435C95BB09DC9720F5B64B25AC7974CD	2/10/2011	2/10/2026
WFA Hotspot 2.0 Intermediate CA	FEA342D00D1A355CF51569EF7E0F617ABB0F22D6D1E73DAA11DCB4D407975543	11/25/2013	11/25/2023
DigiCert CN RSA EV CA G1	B131905CC7221270613B529AC9E786AA230ABFE154A0ACBE452BC350BD1EFE4B	6/20/2019	6/20/2029
DigiCert CN RSA CA G1	03CE9BC71B91FDB7CB3C5235CAE0701CB486BBD628D4AADE5841FC5F0AA37A46	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
DigiCert Global CA-2 G2	1C00D61F6C7EDCB375553C5D1BE1A0EC1F94A4BB24E1A7A50241A556CD74F3A0	10/16/2019	10/16/2029



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

101 South Hanley Road, Suite 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 its CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its 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 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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#). DigiCert’s management is responsible for its assertions. 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 judgement, 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 disclosed in the Mozilla Bugs listed below that certificates were issued with underscore characters in the <code>dnsName</code> , which violates RFC 5280. DigiCert did not revoke all of the certificates impacted by these circumstances in the timelines required by the Baseline Requirements. <ul style="list-style-type: none"><li>- <a href="#">Mozilla Bug 1516599</a></li><li>- <a href="#">Mozilla Bug 1517617</a></li><li>- <a href="#">Mozilla Bug 1519572</a></li><li>- <a href="#">Mozilla Bug 1515788</a></li><li>- <a href="#">Mozilla Bug 1516561</a></li></ul>
		DigiCert created a subordinate CA that did not include the <code>Key Id</code> field of the Authority Key Identifier extension. This does not conform to section 4.2.1.1 of RFC 5280.
2	Log Reviews	Log reviews were performed throughout the audit period using an automated process of monitoring and alerting. The primary long-term storage and retention location of logs is offline. Offline storage locations were not being reviewed for compliance with retention requirements.



Matter Topic		Matter Description
3	System Access Reviews	System access reviews were performed at the network and physical access levels. For the first three quarters of the engagement period, access reviews did not include application level access or offline systems in the scope of the review.
4	Vulnerability Scanning	During the period DigiCert changed the software tool used to perform vulnerability scanning. Due to the tool change, vulnerability scan results of Certificate Systems could not be provided for the period November 2018 to March 2019. BDO was not able to reconcile vulnerabilities identified to remediation actions taken.

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 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 - SSL Baseline with Network Security 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 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) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G3	EB04CF5EB1F39AFA762F2BB120F296CBA520C1B97DB1589565B81CB9A17B7244	10/1/1999	7/16/2036
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



Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
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	D9BC973F88909696DA10833197944CA58AC4A88847779C9133374267100EEC58	11/8/2006	11/7/2021
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	61436A4ED63E31F22EEFAC26B525796CF5EBF89A77E73C0ADCC84DE979B1C5E0	11/5/2007	5/11/2020
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	FB2BD3598144356DCBD2B259E8F3EBD0B0F6EE180C15EF553B82D199EF07F39A	4/2/2008	12/10/2019
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	1512DFAEDF9153FFACB70BC805BA32CB6F9CB3D095B64E6659E652C3CA335A32	4/2/2008	12/10/2019
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	C9D89EC4FC9CAC1E49432294E8A7AA30117AB3E4E0199B9E297D6BE10FC6E2DF	4/2/2008	12/10/2019
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=DigiCert Universal Transition Root	88A07073D4527069DC9E978053F35729705C058302648ED02E5FCE6561459E61	12/8/2017	12/7/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G3	53A5E32ACC5714ED20C7778C655D1EE97EC07156074C8B016E2CFC73E9D2712B	11/6/2017	11/5/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Transition ECC Root	DB98194E55B936D26E6CB3F460A262EB6CA66337E7BFF17A0BFC083251F63626	11/6/2017	11/5/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Transition RSA Root	0D88900DBB68C6CA5471F653FCACD407EBD7B1519046F9E0B8CED3C274FD11A1	11/6/2017	11/5/2022



Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=DigiCert Transition Root G3	0F57B96FA7B31247EC39CB307D38CA2BF3B29F54AFD50A351D18533529517B46	12/8/2017	12/7/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G2	2D4FAD3455AB61397401ABBB518922F84336B67E02FC8D2DB283825C4AB981BB	11/6/2017	11/5/2022

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Netflix, Inc., CN=Netflix Public SHA2 RSA CA 1	227AC6E5AEBB0A356D4C87317CC8CD683D1C4C67129CEE2AA394AD38C0725C93	8/1/2019	12/31/2024
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 Secure Server CA - G4	59F8CB7D7E9E13CB778FF62198EBE05551B515A58BBBA2EF19C33C760C823916	10/31/2013	10/30/2023
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)09, CN=VeriSign Class 3 Secure Server CA - G2	0E48FE8DF79836EF811C61B36EA2C5470531AE80041DB64D29B694B4A1C1BE1F	3/25/2009	3/24/2019
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)09, CN=VeriSign Class 3 Secure Server CA - G2	0A4151D5E58B84B8ACE53A5C12122AC959CD6991FBB38E99B576C0ABDAC35814	3/26/2009	3/24/2019
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 Secure Server CA - G4	564DBC6A76550FD2D4F4BAC6448A1157B33CBD8E0B3FD76D72107540964A85B5	10/31/2013	10/30/2023
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	EAE72EB454BF6C3977EBD289E970B2F5282949190093D0D26F98D0F0D6A9CF17	10/31/2013	10/30/2023
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, OU=Domain Validated SSL, CN=Symantec Basic DV SSL CA - G1	526E30DED6BF9D5CE216F50C832402B48AB70D55AEDA918A1873A5883EBDB1B5	6/7/2016	6/6/2026
C=US, O=Symantec Corporation, OU=Symantec Trust Network, OU=Domain Validated SSL, CN=Symantec Basic DV SSL CA - G2	DFF583E3A1ED35E57D95104817AD823C055FB9071CD400435B5FC74E692081DB	6/7/2016	6/6/2026
C=CN, O=TrustAsia Technologies, Inc., OU=Symantec Trust Network, OU=Domain Validated SSL, CN=TrustAsia DV SSL CA - G5	B41AB845CAB4DB9CB1FE6505765F36A0868ADC5DF419B38979FB6A4FE4131F70	8/11/2016	8/10/2026
C=CN, O=TrustAsia Technologies, Inc., OU=Symantec Trust Network, OU=Domain Validated SSL, CN=TrustAsia DV SSL CA - G6	B90E17AB4B8778B10F9F28CBAA7664DE2EE3D66E1AFC574D168EDD24A10339FF	8/11/2016	8/10/2026



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 - G4	31862233620E789330CC893E8B5E66705331B8888B0ED30A44574D9E0A71C4F1	1/7/2016	1/6/2026
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA	ADEBF83FD3D3F9546BB77FAAB516DD9337CCF91E1198F74337769EC68E6E826E	12/20/2012	12/19/2022
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA - G2	3B6D701331A8CB809443E42A732BAD675F225B15CC439ACF26A09587C885ECFD	5/12/2015	5/11/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA - G2	74EB307A78AC7E8570CC1BAE1C51102A6053C96F3332D703285A743BCBD35D9E	5/12/2015	5/11/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA - G2	2E2861289B5CCEDECAE4C31BF262E0FB0C29B6C1530573442731CA65D821E901	5/12/2015	5/11/2025
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	4B2CBA18EFBCE6C3C4A80AAAABC952337000CD9346B768D062412A2DED846EDC9	1/7/2016	1/6/2026
C=CN, O=TrustAsia Technologies, Inc., OU=Symantec Trust Network, OU=Domain Validated SSL, CN=TrustAsia ECC DV SSL CA - G7	AD806A9357B87D1EB1DD85A5A3C092D0204BA447FF4B3714E3F1034F4D3DE8A0	12/13/2016	12/12/2026



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 384 bit SSL CA	14214583E5F49CE2DB88B93CFE3F7D81B678C86AFBCA9240BAA4B9E4CE90BF2C	12/20/2012	12/19/2022
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
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 Secure Server CA - T1	2C31A92DB8889132E04AD5F43DAF6D421B854510C61E41C787CB5E10E0962DC7	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 International Server CA - T1	F74DA4D9A687C5046499AEFC9FA867DE91A1A3941A09F24CF94603B7AB78108A	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 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=Thawte, Inc., CN=Thawte SGC CA - G2	0CEBF97D1FABC64753799F7A9A508C7C5F2B58B928FB1B3CDC6C4109C0CF2E99	7/29/2010	7/28/2020
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=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 3 MPKI Secure Server CA, CN=Oracle SSL CA	C76F70980598C66A8E327E17B495A2276265C4B9A3575EFA1D550502A823D591	10/12/2010	10/11/2020



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
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
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server SHA256 SSL CA	E0898AD662474B9F753C79BEA878031C9A5D634A49EDD6310B960AB023C02C0E	4/9/2013	4/8/2023
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 Secure Server CA - G3	5B9F350C2A76BE64BB3C2C6E2A414AEDDD0EF0A26D7C97FA7AF57D520C60B2E9	2/8/2010	2/7/2020
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 Secure Server CA - G3	64903546A58058D1E6F1BEAD1134EDE66A6831D231F0DF8D4E28535D7A300496	2/8/2010	2/7/2020
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 Secure Server CA - G3	31DC82EA8915E27D03BBD0433658A3C24C6D3ACFF48C4FAAC02FE87E94C99A3B	2/8/2010	2/7/2020
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 International Server CA - G3	6E21876CF16347201F637A178CB42B171D52379AF7E5F5B6F6755B3EE9BB2ED4	2/8/2010	2/7/2020
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 International Server CA - G3	330260A69C0887F1B9A498302AECFDA17DE89A819C7E57E28C40A53080BE10E8	2/8/2010	2/7/2020





## DIGICERT, INC. MANAGEMENT’S ASSERTION

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

DigiCert management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (“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 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 SSL certificates in conformity with the CA/Browser Forum Requirements on the DigiCert [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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#).

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



Mozilla Bug #	Description	Date Opened	Date Closed
<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
<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



Mozilla Bug #	Description	Date Opened	Date Closed
<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) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G3	EB04CF5EB1F39AFA762F2BB120F296CBA520C1B97DB1589565B81CB9A17B7244	10/1/1999	7/16/2036
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



Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
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	D9BC973F88909696DA10833197944CA58AC4A88847779C9133374267100EEC58	11/8/2006	11/7/2021
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	61436A4ED63E31F22EEFAC26B525796CF5EBF89A77E73C0ADCC84DE979B1C5E0	11/5/2007	5/11/2020
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	FB2BD3598144356DCBD2B259E8F3EBD0B0F6EE180C15EF553B82D199EF07F39A	4/2/2008	12/10/2019
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	1512DFAEDF9153FFACB70BC805BA32CB6F9CB3D095B64E6659E652C3CA335A32	4/2/2008	12/10/2019
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority	C9D89EC4FC9CAC1E49432294E8A7AA30117AB3E4E0199B9E297D6BE10FC6E2DF	4/2/2008	12/10/2019
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=DigiCert Universal Transition Root	88A07073D4527069DC9E978053F35729705C058302648ED02E5FCE6561459E61	12/8/2017	12/7/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G3	53A5E32ACC5714ED20C7778C655D1EE97EC07156074C8B016E2CFC73E9D2712B	11/6/2017	11/5/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Transition ECC Root	DB98194E55B936D26E6CB3F460A262EB6CA66337E7BFF17A0BFC083251F63626	11/6/2017	11/5/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Transition RSA Root	0D88900DBB68C6CA5471F653FCACD407EBD7B1519046F9E0B8CED3C274FD11A1	11/6/2017	11/5/2022



Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=DigiCert Transition Root G3	0F57B96FA7B31247EC39CB307D38CA2BF3B29F54AFD50A351D18533529517B46	12/8/2017	12/7/2022
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G2	2D4FAD3455AB61397401ABBB518922F84336B67E02FC8D2DB283825C4AB981BB	11/6/2017	11/5/2022

Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Netflix, Inc., CN=Netflix Public SHA2 RSA CA 1	227AC6E5AEBB0A356D4C87317CC8CD683D1C4C67129CEE2AA394AD38C0725C93	8/1/2019	12/31/2024
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 Secure Server CA - G4	59F8CB7D7E9E13CB778FF62198EBE05551B515A58BBBA2EF19C33C760C823916	10/31/2013	10/30/2023
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)09, CN=VeriSign Class 3 Secure Server CA - G2	0E48FE8DF79836EF811C61B36EA2C5470531AE80041DB64D29B694B4A1C1BE1F	3/25/2009	3/24/2019
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)09, CN=VeriSign Class 3 Secure Server CA - G2	0A4151D5E58B84B8ACE53A5C12122AC959CD6991FBB38E99B576C0ABDAC35814	3/26/2009	3/24/2019
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G2	6C66B76E68D6C79FAFE5C94E9B7D0CF753C715CC85387E11323B7935F861C187	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 CA - G3	9E6BC5F9ECC52460E8EDC02C644D1BE1CB9F2316F41DAF3B616A0B2058294B31	10/31/2013	10/30/2023
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	564DBC6A76550FD2D4F4BAC6448A1157B33CBD8E0B3FD76D72107540964A85B5	10/31/2013	10/30/2023
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	EAE72EB454BF6C3977EBD289E970B2F5282949190093D0D26F98D0F0D6A9CF17	10/31/2013	10/30/2023
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, OU=Domain Validated SSL, CN=Symantec Basic DV SSL CA - G1	526E30DED6BF9D5CE216F50C832402B48AB70D55AEDA918A1873A5883EBDB1B5	6/7/2016	6/6/2026
C=US, O=Symantec Corporation, OU=Symantec Trust Network, OU=Domain Validated SSL, CN=Symantec Basic DV SSL CA - G2	DF583E3A1ED35E57D95104817AD823C055FB9071CD400435B5FC74E692081DB	6/7/2016	6/6/2026
C=CN, O=TrustAsia Technologies, Inc., OU=Symantec Trust Network, OU=Domain Validated SSL, CN=TrustAsia DV SSL CA - G5	B41AB845CAB4DB9CB1FE6505765F36A0868ADC5DF419B38979FB6A4FE4131F70	8/11/2016	8/10/2026





Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=CN, O=TrustAsia Technologies, Inc., OU=Symantec Trust Network, OU=Domain Validated SSL, CN=TrustAsia DV SSL CA - G6	B90E17AB4B8778B10F9F28CBAA7664DE2EE3D66E1AFC574D168EDD24A10339FF	8/11/2016	8/10/2026
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=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA	ADEBF83FD3D3F9546BB77FAAB516DD9337CCF91E1198F74337769EC68E6E826E	12/20/2012	12/19/2022
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA - G2	3B6D701331A8CB809443E42A732BAD675F225B15CC439ACF26A09587C885ECFD	5/12/2015	5/11/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA - G2	74EB307A78AC7E8570CC1BAE1C51102A6053C96F3332D703285A743BCBD35D9E	5/12/2015	5/11/2025
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 256 bit SSL CA - G2	2E2861289B5CCEDECAE4C31BF262E0FB0C29B6C1530573442731CA65D821E901	5/12/2015	5/11/2025
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



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=CN, O=TrustAsia Technologies, Inc., OU=Symantec Trust Network, OU=Domain Validated SSL, CN=TrustAsia ECC DV SSL CA - G7	AD806A9357B87D1EB1DD85A5A3C092D0204BA447FF4B3714E3F1034F4D3DE8A0	12/13/2016	12/12/2026
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 ECC 384 bit SSL CA	14214583E5F49CE2DB88B93CFE3F7D81B678C86AFBCA9240BAA4B9E4CE90BF2C	12/20/2012	12/19/2022
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
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 Secure Server CA - T1	2C31A92DB8889132E04AD5F43DAF6D421B854510C61E41C787CB5E10E0962DC7	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 International Server CA - T1	F74DA4D9A687C5046499AEFC9FA867DE91A1A3941A09F24CF94603B7AB78108A	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 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=Thawte, Inc., CN=Thawte SGC CA - G2	0CEBF97D1FABC64753799F7A9A508C7C5F2B58B928FB1B3CDC6C4109C0CF2E99	7/29/2010	7/28/2020
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



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 3 MPKI Secure Server CA, CN=Oracle SSL CA	C76F70980598C66A8E327E17B495A2276265C4B9A3575EFA1D550502A823D591	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
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server SHA256 SSL CA	E0898AD662474B9F753C79BEA878031C9A5D634A49EDD6310B960AB023C02C0E	4/9/2013	4/8/2023
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 Secure Server CA - G3	5B9F350C2A76BE64BB3C2C6E2A414AEDDD0EF0A26D7C97FA7AF57D520C60B2E9	2/8/2010	2/7/2020
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 Secure Server CA - G3	64903546A58058D1E6F1BEAD1134EDE66A6831D231F0DF8D4E28535D7A300496	2/8/2010	2/7/2020
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 Secure Server CA - G3	31DC82EA8915E27D03BBD0433658A3C24C6D3ACFF48C4FAAC02FE87E94C99A3B	2/8/2010	2/7/2020
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 International Server CA - G3	6E21876CF16347201F637A178CB42B171D52379AF7E5F5B6F6755B3EE9BB2ED4	2/8/2010	2/7/2020
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 International Server CA - G3	330260A69C0887F1B9A498302AECFDA17DE89A819C7E57E28C40A53080BE10E8	2/8/2010	2/7/2020



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 its CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its 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 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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#). 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 judgement, 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 disclosed in the Mozilla Bugs listed below that certificates were issued with underscore characters in the dNSName, which violates RFC 5280. DigiCert did not revoke all of the certificates impacted by these circumstances in the timelines required by the Baseline Requirements. <ul style="list-style-type: none"><li>- <a href="#">Mozilla Bug 1516599</a></li><li>- <a href="#">Mozilla Bug 1517617</a></li><li>- <a href="#">Mozilla Bug 1519572</a></li><li>- <a href="#">Mozilla Bug 1515788</a></li><li>- <a href="#">Mozilla Bug 1516561</a></li></ul>
2	Log Reviews	Log reviews were performed throughout the audit period using an automated process of monitoring and alerting. The primary long-term storage and retention location of logs is offline. Offline storage locations were not being reviewed for compliance with retention requirements.
3	System Access Reviews	System access reviews were performed at the network and physical access levels. For the first three quarters of the engagement period, access reviews did not include application level access or offline systems in the scope of the review.



Matter Topic		Matter Description
4	Vulnerability Scanning	During the period DigiCert changed the software tool used to perform vulnerability scanning. Due to the tool change, vulnerability scan results of Certificate Systems could not be provided for the period November 2018 to March 2019. BDO was not able to reconcile vulnerabilities identified to remediation actions taken.

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 or Verisign'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 or Verisign's services for any customer's intended purpose.

DigiCert's use of the WebTrust for Certification Authorities - SSL Baseline with Network Security 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., CN=GeoTrust Universal CA 2	A0234F3BC8527CA5628EEC81AD5D69895DA5680DC91D1CB8477F33F878B95B0B	3/4/2004	3/4/2029
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
C=US, O=GeoTrust Inc., CN=GeoTrust Global CA	FF856A2D251DCD88D36656F450126798CFABAAD40799C722DE4D2B5DB36A73A	5/21/2002	5/21/2022
C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2	CA2D82A08677072F8AB6764FF035676CFE3E5E325E012172DF3F92096DB79B85	3/4/2004	3/4/2019
C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA	A0459B9F63B22559F5FA5D4C6DB3F9F72FF19342033578F073BF1D1B46CBB912	3/4/2004	3/4/2029

Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=GeoTrust Primary Transition Root	F54F6CED56CF682B570A6CAEC313E9482760DE12E8F928AE30452C4C66AC761A	12/8/2017	12/7/2022





Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=CH, O=Hostpoint AG, OU=Domain Validated SSL, CN=Hostpoint DV SSL CA - G1	9F4E3C42FATEDA3CF88C05CC4B4AF0C0AF306415C30D3D1EEBEDEBF7D177A982	1/19/2016	1/18/2026
C=CH, O=Hostpoint AG, OU=Domain Validated SSL, CN=Hostpoint DV SSL CA - G2	ABD6D053FDBE356D075050181586B0B9C2B8C03298ABCE64CE25C40401DF3B22	1/19/2016	5/20/2022
C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validated SSL, CN=TrustAsia Technologies, Inc. DV SSL CA - G1	3997C721893B3926D3938A311CA07A261B2AE22E01DC587F181DFF15B98B4EA6	4/5/2016	4/4/2026
C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validated SSL, CN=TrustAsia Technologies, Inc. DV SSL CA - G2	C18949E3659FF7DF22B30EC4DA6B4341AF8BEE00E4177A7F86FF59BC46B6BA40	4/5/2016	5/20/2022
C=DE, O=CertCenter AG, OU=Domain Validated SSL, CN=AlwaysOnSSL CA - G1	EF4478EB094C48FB9FEACA09736270499CA52EB04E3F8EE4C1B2EDC9960398FD	2/16/2016	2/15/2026
C=DE, O=CertCenter AG, OU=Domain Validated SSL, CN=AlwaysOnSSL CA - G2	7D89AE918B25AFDF91036EEE5C15E58C600F42266866A8DE01C71DBC635CA1C0	2/16/2016	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL	2E7E65BB1A013DAF0BDF6938502E43E38217FE00D76CA2F99F7AA9E298F48534	8/6/2013	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G2	78DC9CA5F4C2913F3FB74AC52DFFFC2300DA5A772FC2B84C53A2E74437EDD20	9/8/2014	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G3	4FD73419046F90868826D581536931D22E54943EBCD059CB7621394D749343C5	6/30/2015	6/29/2025



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G4	BC3F0ADC5FF86A4B374DC691F8FE273B1B87DC73E43824F5FE7F36C3E0008311	12/17/2015	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G5	8C88BA510529B64263CCB21A73D82BA5725A55C1446F2547BCE301FCDC4314DB	12/17/2015	12/16/2025
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA	123465EEC4092F8CF7ABFE92B8C701AC09EA79A498F1D3F6A02C1714F39A8423	8/12/2009	5/19/2022
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA	32251B9BB3D76421D3B300FCED4757EEE04167A727904AC188B35111D261F56	8/11/2009	5/20/2022
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA - G2	F7AE9B5870DCDA431905AEA03B3993A34E877B876B784152817F1C58657E37C4	2/10/2015	5/19/2022
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA - G2	56CBB0FFC414E88822A50E9F42D46820381D8C2AAEEF56E0566817ED30F27A27	2/10/2015	5/19/2022
C=NL, O=Intermediate Certificate, OU=Domain Validated SSL, CN=Intermediate Certificate DV SSL CA	8C2745352289E994B3EA349445B1CF6418E51740E1614F8B5667DAD2990AAEFB	6/1/2012	5/21/2022
C=NL, O=Intermediate Certificate, OU=Domain Validated SSL, CN=Intermediate Certificate DV SSL CA - G2	D876A081FB3827BA22A4087DF675126FF8A96AAB90364BC61F62CE8E9507AA93	9/8/2014	5/20/2022
C=NL, O=Intermediate Certificate, OU=Domain Validated SSL, CN=Intermediate Certificate DV SSL CA - G3	E86BC16CC6491E5F4B9976313842B3D02C99EA263AEB1DC223D898FA87C84845	6/30/2015	6/29/2025



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=NL, O=Trust Provider B.V., OU=Domain Validated SSL, CN=Trust Provider B.V. DV SSL CA - G1	D6EA1061C28B3DB96FF5BAA140AB5714E6B0B4F5D71ABCCD242A49B9B9F4DC27	1/21/2016	1/20/2026
C=NL, O=Trust Provider B.V., OU=Domain Validated SSL, CN=Trust Provider B.V. DV SSL CA - G2	81051C355EC9F5A89FBA91D1A5BD3F0501EACD80EF93B218003D95CF251A7670	1/21/2016	5/20/2022
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 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
C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SHA256 SSL CA	BC9E223CC42275CC034190DF2D0179B55B732D5AC531137A7B522DCFE04A0592	4/9/2013	4/8/2023
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 SHA256 SSL CA	D9E0C64AB27A64D79CCCF42A34EC75A251A7E543353C19E984A70EB2F546CDFF	5/23/2013	5/22/2023



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G2	90AF11E577C72C940B40EC2F3D50507310091EE6196C9C16B228882264A4D808	8/27/2012	5/20/2022
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G2	5F7C89EB8698C20E5BA9EA23F0D12EDBC8DB1E1D276264B0D4D159A0DEDFBD8F	8/24/2012	5/20/2022
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3	074541ECDF88ED992ED5ADE3ECDDEF27A26BA1B44480A195C0A8DADAE2521D8E	11/5/2013	5/20/2022
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G4	211DDF5059229B3577760D623D5148DB92F2D0526EA5303E7EEA0300D9FAFF3F	9/8/2014	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL CA - G2	0DCDC07ECABBBFE38A4606BA663987CDB3BD9817FC67D1DD0CF094AC8CA2787D	6/5/2013	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA	E6683E88315CD1CB403C0CEA490F7C4B4C82C91CD485037489AADBAA90839F61	12/11/2013	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G2	92EF2F5B553570607DC29C8010E7ABC16283FE355F955A248254290A260A9EBB	6/10/2014	6/9/2024
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3	BC3F03A436240EDBA5F83714F6F677E34B37F9B1F0C08C1E558D981E279E8209	8/29/2014	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G4	5B87E222F20346FA3628816ED6CE71FAABA0857FB8BCBA73776EA1FA56CD0057	6/30/2015	6/29/2025



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA	C27FD4B85E96D3777C68AB7DF6AA4E626BF3FF8C72B1CE81D1EB78BABEB1A074	2/26/2010	2/25/2020
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA - G2	DEDB31CBCEC5F99D38E86ECC4D76945DF40F2E547C94E4B0124094875AF6A558	6/4/2013	5/20/2022
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA - G3	51CF0FFFC3253FC013AF786F95B190109F8C87F34DFD1CEC44C45888789F5355	6/11/2014	5/20/2022
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA - G4	8BC1B9D7DEFCCA1CCD09BACDA88F27762092F1ED4A34AE5E4602BB9CC915C506	8/29/2014	5/20/2022
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL SHA256 CA	784ACA1063BE4700B3A62F45C2F93B7EEF8BF230FB869610E864FC4B3A23D09F	6/10/2014	6/9/2024
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL SHA256 CA - G2	3FDF788A5A65E6A29D8C1550D8244906A3B8A7B7D3DA9BDEDD748E4183A763C9	6/30/2015	6/29/2025
C=US, O=GeoTrust Inc., OU=GeoTrust Authentication Services, CN=GeoTrust True Identity CA 2	FF1D35ED464063D6031C71E414262CC2310E8C547AB7F7CF2955C9E0349E533F	1/28/2011	1/25/2021
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 SSL CA	D4C4C99819F3A5F2C6261C9444C62A8B263B39BC6ACCE35CDCABE272D5037FB2	2/19/2010	2/18/2020



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust, Inc., CN=GeoTrust True Credentials CA 3	5D74ED61D0B311E981BBCF0F419A35FA9FA1EC70FF1AEB742D73BCFEBA06CFFF	8/22/2012	5/21/2022
C=US, O=GeoTrust, Inc., CN=RapidSSL CA	6D5BC979461C7264E1710010CD7D4EA3EC57FA11215F04FFA516AE61959AB2B2	2/19/2010	2/18/2020
C=US, O=GeoTrust, Inc., OU=Domain Validated SSL, CN=GeoTrust Secure Site Starter DV SSL CA - G1	62FB9B6CD2633B92D91DB264CE678A9B19C575414AB10AD46D157F07BBA26EFF	9/1/2015	8/31/2025
C=US, O=GeoTrust, Inc., OU=Domain Validated SSL, CN=Secure Site Starter DV SSL CA - G2	64853613C2436399603D0D560B52F04BB8F81A81746E42389883A4F59A4564D5	12/1/2015	11/30/2025
C=US, O=GeoTrust, Inc., OU=Domain Validated SSL, CN=Secure Site Starter DV SSL CA - G3	2FCC009AAFDB28E9256430410A6FA6E76AF09301B1044FEAAACAB00215AA39E1	12/1/2015	5/20/2022
C=US, O=GeoTrust, Inc., OU=For Internal Use Only, CN=RapidSSL Enterprise CA	2A400E478B9F56C13762A49754144B6B8C4A5A1DC8E7B31E441D0DBD1A6A4BE4	3/8/2011	3/5/2021
C=US, O=GeoTrust, Inc., OU=For Internal Use Only, CN=RapidSSL Enterprise CA	87AA71AF032E36BD69DAF4014FCAD8F2733AA00DEAB959335AE3866E4B6D3A1D	3/8/2011	3/5/2021
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA	8FDA7A8813546F9A7CB065CD32D3650D5B56A2B7F942B9499AEB42A86A3E9D56	4/11/2011	4/8/2021
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G2	6FF6F63F6A0D3D63446CDAA523D26273B126C02F922E05D73C4748EB89B86393	9/8/2014	5/20/2022



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G3	80D9EDB45B7F592CD30254E55BC316BBF44E47DFC0C004A383281C03F345BA39	6/30/2015	6/29/2025
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G4	ED67937083B0739F302396F974AFB41BFBA648473967780B2C59B88AC4121AD4	12/17/2015	5/20/2022
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G5	9FE306E663E459644644F60A7153A221436FB9701A0EBD9124EEF8159D15CB43	12/17/2015	12/16/2025
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 International Server CA - G3	6E21876CF16347201F637A178CB42B171D52379AF7E5F5B6F6755B3EE9BB2ED4	2/8/2010	2/7/2020
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 International Server CA - G3	330260A69C0887F1B9A498302AECFDA17DE89A819C7E57E28C40A53080BE10E8	2/8/2010	2/7/2020



## DIGICERT, INC. MANAGEMENT’S ASSERTION

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

DigiCert management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its 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 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 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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#).

We noted the following other matters during our procedures:

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





Mozilla Bug #	Description	Date Opened	Date Closed
<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
<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



Mozilla Bug #	Description	Date Opened	Date Closed
<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 over 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., CN=GeoTrust Universal CA 2	A0234F3BC8527CA5628EEC81AD5D69895DA5680DC91D1CB8477F33F878B95B0B	3/4/2004	3/4/2029
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
C=US, O=GeoTrust Inc., CN=GeoTrust Global CA	FF856A2D251DCD88D36656F450126798CFABAAD40799C722DE4D2B5DB36A73A	5/21/2002	5/21/2022
C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2	CA2D82A08677072F8AB6764FF035676CFE3E5E325E012172DF3F92096DB79B85	3/4/2004	3/4/2019
C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA	A0459B9F63B22559F5FA5D4C6DB3F9F72FF19342033578F073BF1D1B46CBB912	3/4/2004	3/4/2029

Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=GeoTrust Primary Transition Root	F54F6CED56CF682B570A6CAEC313E9482760DE12E8F928AE30452C4C66AC761A	12/8/2017	12/7/2022



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=CH, O=Hostpoint AG, OU=Domain Validated SSL, CN=Hostpoint DV SSL CA - G1	9F4E3C42FAFEDA3CF88C05CC4B4AF0C0AF306415C30D3D1EEBEDEBF7D177A982	1/19/2016	1/18/2026
C=CH, O=Hostpoint AG, OU=Domain Validated SSL, CN=Hostpoint DV SSL CA - G2	ABD6D053FDBE356D075050181586B0B9C2B8C03298ABCE64CE25C40401DF3B22	1/19/2016	5/20/2022
C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validated SSL, CN=TrustAsia Technologies, Inc. DV SSL CA - G1	3997C721893B3926D3938A311CA07A261B2AE22E01DC587F181DFF15B98B4EA6	4/5/2016	4/4/2026
C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validated SSL, CN=TrustAsia Technologies, Inc. DV SSL CA - G2	C18949E3659FF7DF22B30EC4DA6B4341AF8BEE00E4177A7F86FF59BC46B6BA40	4/5/2016	5/20/2022
C=DE, O=CertCenter AG, OU=Domain Validated SSL, CN=AlwaysOnSSL CA - G1	EF4478EB094C48FB9FEACA09736270499CA52EB04E3F8EE4C1B2EDC9960398FD	2/16/2016	2/15/2026
C=DE, O=CertCenter AG, OU=Domain Validated SSL, CN=AlwaysOnSSL CA - G2	7D89AE918B25AFDF91036EEE5C15E58C600F42266866A8DE01C71DBC635CA1C0	2/16/2016	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL	2E7E65BB1A013DAF0BDF6938502E43E38217FE00D76CA2F99F7AA9E298F48534	8/6/2013	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G2	78DC9CA5F4C2913F3FB74AC52DFFFC2300DA5A772FC2B84C53A2E74437EDD20	9/8/2014	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G3	4FD73419046F90868826D581536931D22E54943EBCD059CB7621394D749343C5	6/30/2015	6/29/2025



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G4	BC3F0ADC5FF86A4B374DC691F8FE273B1B87DC73E43824F5FE7F36C3E0008311	12/17/2015	5/20/2022
C=DE, O=STRATO AG, OU=Domain Validated SSL, CN=STRATO SSL - G5	8C88BA510529B64263CCB21A73D82BA5725A55C1446F2547BCE301FCDC4314DB	12/17/2015	12/16/2025
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA	123465EEC4092F8CF7ABFE92B8C701AC09EA79A498F1D3F6A02C1714F39A8423	8/12/2009	5/19/2022
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA	32251B9BB3D76421D3B300FCED4757EEE04167A727904AC188B351111D261F56	8/11/2009	5/20/2022
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA - G2	F7AE9B5870DCDA431905AEA03B3993A34E877B876B784152817F1C58657E37C4	2/10/2015	5/19/2022
C=JP, O=NTT DOCOMO, INC., OU=GeoRoot Certification Authority, CN=DKHS Device CA - G2	56CBB0FFC414E88822A50E9F42D46820381D8C2AAEEF56E0566817ED30F27A27	2/10/2015	5/19/2022
C=NL, O=Intermediate Certificate, OU=Domain Validated SSL, CN=Intermediate Certificate DV SSL CA	8C2745352289E994B3EA349445B1CF6418E51740E1614F8B5667DAD2990AAEFB	6/1/2012	5/21/2022
C=NL, O=Intermediate Certificate, OU=Domain Validated SSL, CN=Intermediate Certificate DV SSL CA - G2	D876A081FB3827BA22A4087DF675126FF8A96AAB90364BC61F62CE8E9507AA93	9/8/2014	5/20/2022
C=NL, O=Intermediate Certificate, OU=Domain Validated SSL, CN=Intermediate Certificate DV SSL CA - G3	E86BC16CC6491E5F4B9976313842B3D02C99EA263AEB1DC223D898FA87C84845	6/30/2015	6/29/2025



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=NL, O=Trust Provider B.V., OU=Domain Validated SSL, CN=Trust Provider B.V. DV SSL CA - G1	D6EA1061C28B3DB96FF5BAA140AB5714E6B0B4F5D71ABCCD242A49B9B9F4DC27	1/21/2016	1/20/2026
C=NL, O=Trust Provider B.V., OU=Domain Validated SSL, CN=Trust Provider B.V. DV SSL CA - G2	81051C355EC9F5A89FBA91D1A5BD3F0501EACD80EF93B218003D95CF251A7670	1/21/2016	5/20/2022
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 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
C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SHA256 SSL CA	BC9E223CC42275CC034190DF2D0179B55B732D5AC531137A7B522DCFE04A0592	4/9/2013	4/8/2023
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 SHA256 SSL CA	D9E0C64AB27A64D79CCCF42A34EC75A251A7E543353C19E984A70EB2F546CDFF	5/23/2013	5/22/2023



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G2	90AF11E577C72C940B40EC2F3D50507310091EE6196C9C16B228882264A4D808	8/27/2012	5/20/2022
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G2	5F7C89EB8698C20E5BA9EA23F0D12EDBC8DB1E1D276264B0D4D159A0DEDFBD8F	8/24/2012	5/20/2022
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3	074541ECDF88ED992ED5ADE3ECDDEF27A26BA1B44480A195C0A8DADAE2521D8E	11/5/2013	5/20/2022
C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G4	211DDF5059229B3577760D623D5148DB92F2D0526EA5303E7EEA0300D9FAFF3F	9/8/2014	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL CA - G2	0DCDC07ECABBBFE38A4606BA663987CDB3BD9817FC67D1DD0CF094AC8CA2787D	6/5/2013	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA	E6683E88315CD1CB403C0CEA490F7C4B4C82C91CD485037489AADBAA90839F61	12/11/2013	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G2	92EF2F5B553570607DC29C8010E7ABC16283FE355F955A248254290A260A9EBB	6/10/2014	6/9/2024
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3	BC3F03A436240EDBA5F83714F6F677E34B37F9B1F0C08C1E558D981E279E8209	8/29/2014	5/20/2022
C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G4	5B87E222F20346FA3628816ED6CE71FAABA0857FB8BCBA73776EA1FA56CD0057	6/30/2015	6/29/2025





Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA	C27FD4B85E96D3777C68AB7DF6AA4E626BF3FF8C72B1CE81D1EB78BABEB1A074	2/26/2010	2/25/2020
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA - G2	DEDB31CBCEC5F99D38E86ECC4D76945DF40F2E547C94E4B0124094875AF6A558	6/4/2013	5/20/2022
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA - G3	51CF0FFFC3253FC013AF786F95B190109F8C87F34DFD1CEC44C45888789F5355	6/11/2014	5/20/2022
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA - G4	8BC1B9D7DEFCCA1CCD09BACDA88F27762092F1ED4A34AE5E4602BB9CC915C506	8/29/2014	5/20/2022
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL SHA256 CA	784ACA1063BE4700B3A62F45C2F93B7EEF8BF230FB869610E864FC4B3A23D09F	6/10/2014	6/9/2024
C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL SHA256 CA - G2	3FDF788A5A65E6A29D8C1550D8244906A3B8A7B7D3DA9BDEDD748E4183A763C9	6/30/2015	6/29/2025
C=US, O=GeoTrust Inc., OU=GeoTrust Authentication Services, CN=GeoTrust True Identity CA 2	FF1D35ED464063D6031C71E414262CC2310E8C547AB7F7CF2955C9E0349E533F	1/28/2011	1/25/2021
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 SSL CA	D4C4C99819F3A5F2C6261C9444C62A8B263B39BC6ACCE35CDCABE272D5037FB2	2/19/2010	2/18/2020



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=GeoTrust, Inc., CN=GeoTrust True Credentials CA 3	5D74ED61D0B311E981BBCF0F419A35FA9FA1EC70FF1AEB742D73BCFEBA06CFFF	8/22/2012	5/21/2022
C=US, O=GeoTrust, Inc., CN=RapidSSL CA	6D5BC979461C7264E1710010CD7D4EA3EC57FA11215F04FFA516AE61959AB2B2	2/19/2010	2/18/2020
C=US, O=GeoTrust, Inc., OU=Domain Validated SSL, CN=GeoTrust Secure Site Starter DV SSL CA - G1	62FB9B6CD2633B92D91DB264CE678A9B19C575414AB10AD46D157F07BBA26EFF	9/1/2015	8/31/2025
C=US, O=GeoTrust, Inc., OU=Domain Validated SSL, CN=Secure Site Starter DV SSL CA - G2	64853613C2436399603D0D560B52F04BB8F81A81746E42389883A4F59A4564D5	12/1/2015	11/30/2025
C=US, O=GeoTrust, Inc., OU=Domain Validated SSL, CN=Secure Site Starter DV SSL CA - G3	2FCC009AAFDB28E9256430410A6FA6E76AF09301B1044FEAAACAB00215AA39E1	12/1/2015	5/20/2022
C=US, O=GeoTrust, Inc., OU=For Internal Use Only, CN=RapidSSL Enterprise CA	2A400E478B9F56C13762A49754144B6B8C4A5A1DC8E7B31E441D0DBD1A6A4BE4	3/8/2011	3/5/2021
C=US, O=GeoTrust, Inc., OU=For Internal Use Only, CN=RapidSSL Enterprise CA	87AA71AF032E36BD69DAF4014FCAD8F2733AA00DEAB959335AE3866E4B6D3A1D	3/8/2011	3/5/2021
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA	8FDA7A8813546F9A7CB065CD32D3650D5B56A2B7F942B9499AEB42A86A3E9D56	4/11/2011	4/8/2021
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G2	6FF6F63F6A0D3D63446CDAA523D26273B126C02F922E05D73C4748EB89B86393	9/8/2014	5/20/2022



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G3	80D9EDB45B7F592CD30254E55BC316BBF44E47DFC0C004A383281C03F345BA39	6/30/2015	6/29/2025
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G4	ED67937083B0739F302396F974AFB41BFBA648473967780B2C59B88AC4121AD4	12/17/2015	5/20/2022
C=US, O=Volusion, Inc., OU=Domain Validated SSL, CN=Volusion, Inc. DV SSL CA - G5	9FE306E663E459644644F60A7153A221436FB9701A0EBD9124EEF8159D15CB43	12/17/2015	12/16/2025
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 International Server CA - G3	6E21876CF16347201F637A178CB42B171D52379AF7E5F5B6F6755B3EE9BB2ED4	2/8/2010	2/7/2020
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 International Server CA - G3	330260A69C0887F1B9A498302AECFDA17DE89A819C7E57E28C40A53080BE10E8	2/8/2010	2/7/2020

## 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 its CAs as enumerated in [Attachment B](#), DigiCert has:

- disclosed its 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 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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#). 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 judgement, 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 disclosed in the Mozilla Bugs listed below certificates were issued with underscore characters in the dNSName, which violates RFC 5280. DigiCert did not revoke all of the certificates impacted by these circumstances in the timelines required by the Baseline Requirements. <ul style="list-style-type: none"><li>- <a href="#">Mozilla Bug 1516599</a></li><li>- <a href="#">Mozilla Bug 1517617</a></li><li>- <a href="#">Mozilla Bug 1519572</a></li><li>- <a href="#">Mozilla Bug 1515788</a></li><li>- <a href="#">Mozilla Bug 1516561</a></li></ul>
2	Log Reviews	Log reviews were performed throughout the audit period using an automated process of monitoring and alerting. The primary long-term storage and retention location of logs is offline. Offline storage locations were not being reviewed for compliance with retention requirements.
3	System Access Reviews	System access reviews were performed at the network and physical access levels. For the first three quarters of the engagement period, access reviews did not include application level access or offline systems in the scope of the review.



Matter Topic		Matter Description
4	Vulnerability Scanning	During the period DigiCert changed the software tool used to perform vulnerability scanning. Due to the tool change, vulnerability scan results of Certificate Systems could not be provided for the period November 2018 to March 2019. BDO was not able to reconcile vulnerabilities identified to remediation actions taken.

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 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 - SSL Baseline with Network Security 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	A4310D50AF18A6447190372A86AFAF8B951FFB431D837F1E5688B45971ED1557	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

Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=thawte Primary G3 Transition Root	85743AEA6A97C13445E0824C2E1FE502B97ADD124A97EF5120FE07F55812FC33	12/8/2017	12/7/2022
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=thawte Primary Transition Root	DBA1097710F3C629943C23DC7503AC82B9142825EF049F1C26538DB36B480549	12/8/2017	12/7/2022

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





Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., CN=thawte EV SSL CA - G2	37F6BD9BEE0C74F608DD474B56A72F8183077DFC2662AF79BFE3D4FABC0B1C4	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
C=US, O=thawte, Inc., CN=thawte SHA256 SSL CA	3F3AF9C9CC2C7599EF8F6DD7CA516CFC1797D7D12002254F3BFD0D4D0FE9DE86	5/23/2013	5/22/2023
C=US, O=Thawte, Inc., CN=Thawte SSL CA	0855414AF5F5FD7E264F8B002A39CCED67E5952E89B61B680CC847BAA34944DE	2/8/2010	2/7/2020
C=US, O=thawte, Inc., CN=thawte SSL CA - G2	B7A8AF2A4A43F0A86B15604DE6461209C9CD76894D8B0748BC99D9A797013BB0	10/31/2013	10/30/2023
C=US, O=Thawte, Inc., OU=Domain Validated SSL, CN=Thawte DV SSL CA	D2573831FA5376B1C7DC0DBB0EF58813E9070618FA5A21E13F5E9F2B65E0A320	2/18/2010	2/17/2020



Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=thawte, Inc., OU=Domain Validated SSL, CN=thawte DV SSL CA - G2	9F2511A23E70D95FB62798508A676CC38964100936A6E6D3CAE77154C0290F02	6/10/2014	6/9/2024
C=US, O=thawte, Inc., OU=Domain Validated SSL, CN=thawte DV SSL SHA256 CA	537C5C8072363E147C84D21D0D2248B6B99A9A8A43311659835EC33926DA2860	6/10/2014	6/9/2024



## DIGICERT, INC. MANAGEMENT’S ASSERTION

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

DigiCert management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its 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 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 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
  - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#).

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



Mozilla Bug #	Description	Date Opened	Date Closed
<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
<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



Mozilla Bug #	Description	Date Opened	Date Closed
<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 Statements 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	8D722F81A9C113C0791DF136A2966DB26C950A971DB46B4199F4EA54B78BF9F	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	A4310D50AF18A6447190372A86AFAF8B951FFB431D837F1E5688B45971ED1557	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

Cross-Signed CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=thawte Primary G3 Transition Root	85743AEA6A97C13445E0824C2E1FE502B97ADD124A97EF5120FE07F55812FC33	12/8/2017	12/7/2022
C=US, O=DigiCert, Inc, OU=www.digicert.com, CN=thawte Primary Transition Root	DBA1097710F3C629943C23DC7503AC82B9142825EF049F1C26538DB36B480549	12/8/2017	12/7/2022



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
C=US, O=thawte, Inc., CN=thawte SHA256 SSL CA	3F3AF9C9CC2C7599EF8F6DD7CA516CFC1797D7D12002254F3BFD0D4D0FE9DE86	5/23/2013	5/22/2023
C=US, O=Thawte, Inc., CN=Thawte SSL CA	0855414AF5F5FD7E264F8B002A39CCED67E5952E89B61B680CC847BAA34944DE	2/8/2010	2/7/2020
C=US, O=thawte, Inc., CN=thawte SSL CA - G2	B7A8AF2A4A43F0A86B15604DE6461209C9CD76894D8B0748BC99D9A797013BB0	10/31/2013	10/30/2023





Class 3 CAs			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Thawte, Inc., OU=Domain Validated SSL, CN=Thawte DV SSL CA	D2573831FA5376B1C7DC0DBB0EF58813E9070618FA5A21E13F5E9F2B65E0A320	2/18/2010	2/17/2020
C=US, O=thawte, Inc., OU=Domain Validated SSL, CN=thawte DV SSL CA - G2	9F2511A23E70D95FB62798508A676CC38964100936A6E6D3CAE77154C0290F02	6/10/2014	6/9/2024
C=US, O=thawte, Inc., OU=Domain Validated SSL, CN=thawte DV SSL SHA256 CA	537C5C8072363E147C84D21D0D2248B6B99A9A8A43311659835EC33926DA2860	6/10/2014	6/9/2024