SCOTT S. PERRY CPA, PLLC
AFFIRMING DIGITAL TRUST

INDEPENDENT CERTIFIED PUBLIC ACCOUNTANT'S REPORT

Dan Timpson
Chief Technology Officer
DigiCert, Inc.

Dear Mr. Timpson:

I have examined the attached assertions by you representing the management of DigiCert, Inc. ("DigiCert") that in providing its Certification Authority ("CA") services in: Lehi, Lindon, and St. George, Utah; Mountain View, California; Melbourne, Australia; Cape Town, South Africa; Dublin, Ireland; and Kawasaki-shi, Sapporo, and Tokyo, Japan during the period from April 1, 2017 through March 31, 2018. DigiCert has:

- Disclosed in its applicable Certificate Policy and Certification Practices Statement, located at https://www.digicert.com/ssl-cps-repository.htm, its certificate practices and procedures and its commitment to provide SSL certificates in conformity with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, and the CA/Browser Forum Network and Certificate Systems Security Requirements;
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated for the registration activities performed by DigiCert; and verified;
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in DigiCert's business practices disclosure;
  - The continuity of key and certificate life cycle management operations was maintained;
  - DigiCert's systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity; and,
  - DigiCert maintained effective controls to meet the aforementioned CA/Browser Forum requirements;

in accordance with the WebTrust® for Certification Authorities Trust Services Principles and Criteria for Certification Authorities–SSL Baseline with Network Security–Version 2.2.

DigiCert management is responsible for its assertion. My responsibility is to express an opinion on management's assertion based on my examination.

My examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included:

- Obtaining an understanding of DigiCert's key and certificate lifecycle management and information privacy practices;
- Obtaining an understanding of DigiCert's controls over:
  - Key and certificate integrity;
  - The authenticity and privacy of subscriber and relying party information;

- The continuity of key and certificate lifecycle management operations; and
- The development, maintenance and operation of CA systems;

- Selectively testing transactions executed in accordance with DigiCert's disclosed key and certificate life cycle management practices;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as I considered necessary in the circumstances.

I believe that my examination provides a reasonable basis for my opinion. The relative effectiveness and significance of specific controls at DigiCert and their effect on assessments of control risk for subscribers and relying party locations are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. I have performed no procedures to evaluate the controls at individual subscriber or relying party locations.

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 my findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In my opinion, for the period from April 1, 2017 through March 31, 2018, DigiCert management's assertions, as described in the first paragraph of this report, are fairly stated, in all material respects, based on the WebTrust® for Certification Authorities Trust Services Principles and Criteria for Certification Authorities–SSL Baseline with Network Security–Version 2.2.

This report does not include any representation as to the quality of DigiCert's services beyond those covered by the aforementioned criteria, nor the suitability of any DigiCert's services for any customer intended purpose.

DigiCert's use of the WebTrust® Principles and Criteria for Certification Authorities–SSL Baseline with Network Seal constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to update this report or provide any additional assurance.

Scott S. Perry CPA, PLLC

Scott S. Perry CPA, PLLC
Bellevue, Washington
April 20, 2018

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from April 1, 2017 through March 31, 2018

April 20, 2018

As set forth in Appendix A, DigiCert, Inc. (DigiCert) operates various Certification Authorities (CAs) that provide a range of CA services, the operations of which are described more fully in DigiCert's Certificate Policy and Certification Practice Statement, located at https://www.digicert.com/ssl-cps-repository.htm.

DigiCert provides the following certification authority services through its CAs:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

Management of DigiCert is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Certification Practice Statement, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to DigiCert's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of DigiCert has assessed the controls over its CA operations. Based on that assessment, in DigiCert Management's opinion, in providing its Certification Authority (CA) services in Lehi, Lindon and St. George, Utah, Mountain View, CA USA, Melbourne, Australia, Dublin, Ireland, Cape Town, South Africa, Kawasaki-shi, Sapporo and Tokyo, Japan, during the period from April 1, 2017, through March 31, 2018, DigiCert has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy and Certification Practices Statement;
- maintained effective controls to provide reasonable assurance that;
  - its Certification Practice Statement is consistent with its Certificate Policy, and
  - it provides its services in accordance with its Certificate Policy and Certification Practices Statement;
- maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly authenticated (for the registration activities performed by DigiCert), and
  - the integrity of keys and certificates it managed was established and protected throughout their life cycles;
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data was restricted to authorized

individuals,
- the continuity of key and certificate life cycle management operations was maintained, and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.2 (WebTrust SSL Baseline with Network Security).

We confirm, to the best of our knowledge and belief, that DigiCert has complied with its disclosed practices and that the disclosed practices comply with WebTrust SSL Baseline with Network Security. DigiCert agrees to:

- Permit Scott S. Perry CPA, PLLC to conduct subsequent examinations at such times as Scott S. Perry CPA, PLLC may deem appropriate to update Scott S. Perry CPA, PLLC's reports and maintain the Scott S. Perry CPA, PLLC Web Seals, but not to exceed 12 months from the date of the reports.
- Maintain internal controls, practices and disclosures that are compliant with WebTrust SSL Baseline with Network Security as they relate to DigiCert's operations.
- Notify Scott S. Perry CPA, PLLC regarding changes affecting the CAs including changes to our internal controls, practices and disclosures or the manner in which they achieve compliance with WebTrust SSL Baseline with Network Security.
- Provide Scott S. Perry CPA, PLLC with an opportunity to review and agree on the presentation of the Scott S. Perry CPA, PLLC Web Seals and reports on our Web site or other marketing materials prior to making such information available to third parties.
- To permit Scott S. Perry CPA, PLLC to unilaterally remove the Scott S. Perry CPA, PLLC Web Seals if:
  - Scott S. Perry CPA, PLLC finds that changes, such as those described above, have been made but not communicated to Scott S. Perry CPA, PLLC by us.
  - A subsequent examination has not been made within 12 months for any reason.
  - During the course of performing the engagement Scott S. Perry CPA, PLLC discover that changes we have made results in practices, which no longer meet the requirements of WebTrust SSL Baseline with Network Security.

Management acknowledges that Scott S. Perry CPA, PLLC's examination was limited to DigiCert's CA systems and does not include other systems, controls, operations or services not specified.

Further, we confirm that we are responsible for the fair presentation of the assertions described in this letter in conformity with WebTrust SSL Baseline with Network Security.

DigiCert, Inc.

Dan Timpson
Chief Technology Officer

APPENDIX A – WEBTRUST FOR CAs – BASELINE REQUIREMENTS SSL/TLS SERVERS – LIST OF CAs IN SCOPE

Self-Signed Root CAs

Subject Common Name	SHA-256 Hash
Baltimore CyberTrust Root	16AF57A9F676B0AB126095AA5EBADEF22AB31119D644AC95CD4B93DBF3F26AEB
Cybertrust Global Root	802447EE521CC666CDB7BBAE93A385E55F200D76A3D1356A85445AC4CBDBED12
Cybertrust Global Root	960ADF0063E96356750C2965DD0A0867DA0B9CBD6E77714AEAFB2349AB393DA3
DigiCert Assured ID Root CA	3E9099B5015E8F486C00BCEA9D111EE721FABA355A89BCF1DF69561E3DC6325C
DigiCert Assured ID Root G2	7D05EBB682339F8C9451EE094EEBFEFA7953A114EDB2F44949452FAB7D2FC185
DigiCert Assured ID Root G3	7E37CB8B4C47090CAB36551BA6F45DB840680FBA166A952DB100717F43053FC2
DigiCert Global Root CA	4348A0E9444C78CB265E058D5E8944B4D84F9662BD26DB257F8934A443C70161
DigiCert Global Root G2	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F
DigiCert Global Root G3	31AD6648F8104138C738F39EA4320133393E3A18CC02296EF97C2AC9EF6731D0
DigiCert High Assurance EV Root CA	7431E5F4C3C1CE4690774F0B61E05440883BA9A01ED00BA6ABD7806ED3B118CF
DigiCert Trusted Root G4	552F7BDCF1A7AF9E6CE672017F4F12ABF77240C78E761AC203D1D9D20AC89988
Hotspot 2.0 Trust Root CA - 03	A3CC68595DFE7E86D8AD1772A8B5284ADD54ACE3B8A798DF47BCCAFB1FDB84DF
Verizon Global Root CA	68AD50909B04363C605EF13581A939FF2C96372E3F12325B0A6861E1D59F6603

Roots Cross-Signed by Other Roots

Subject Common Name	SHA-256 Hash
Cybertrust Global Root	24905145BD9B9BFE99C60354B49951BE0E709F1634CFBD0E370FEB9F068ED6C3
Cybertrust Global Root	64B3542D1BC972F58A1D179F3D0B9652BE434F3AE3842E0C447880D4D623A4DE
Cybertrust Global Root	9BB5CC8427AF276BF216A748AD25785D17ACBABDDE4282E606DA5262CD940F38
Cybertrust Global Root	9F61D09768DA33F7F99F7E7EAD935902224943B4C9AD07B629F745C0B08475B7
Cybertrust Global Root	D775784887CDBD7E9FCB2A9D589D367A0B6238DA1EAF51DC71C99B89B99229E0
Cybertrust Global Root	E71D8C3BAF43F6B3352DF574A9F0D4A2065BF03DA179514B1FCC5D9BEC8C8FCD
DigiCert Global Root CA	6DACBB8945137B1DAD4211B0436EFBE06F12ACE36904973B45AE25740823D369
DigiCert Global Root G2	2D4FAD3455AB61397401ABBB518922F84336B67E02FC8D2DB283825C4AB981BB
DigiCert Global Root G2	AADADD5A879D2EB8C41A89597291292709D42052F5B6399541C694C3B7353CD1
DigiCert Global Root G3	53A5E32ACC5714ED20C7778C655D1EE97EC07156074C8B016E2CFC73E9D2712B
DigiCert High Assurance EV Root CA	89DAADB41BA698BB378AEE84EAC96121D20F8C2FCA63EC686D9307229AD3EB2E
DigiCert High Assurance EV Root CA	BF0ADF6F1FD218CFA27F3884CE2AA6AF2AF5481C6878BFE3A6CA62515898B115
DigiCert High Assurance EV Root CA	CBF8FB77660167E6BAACD0DF77CDA397D0117EE2BEEA23B935317F8BB5B5E3B0
DigiCert Trusted Root G4	AD8EB32C9DA91DDC855F382745990147DC6F23D9FBB04FC9D476B1EE20FC71D8
Verizon Global Root CA	B90EEAE931E5E2B7D335F149DA6C2210986000D214FFDB62A72F7332D63731AF
Verizon Global Root CA	D96CBC03B523CD3315918651CF4862162887DD563AFB2352D3F34BB94576F93D

Subordinate CAs

Subject Common Name	SHA-256 Hash
AAMC Direct Intermediate CA	BB1C01E884DD0919AB94D5AF5575CD6FEB71E560B2B58735A78B150A10D54BF3
Abbott Laboratories Secure Authentication CA	DB99A4F284CCF10B26DE7B7A5D651725B857CBC871EBB33028D67B55510EFCD9
Abbott Laboratories Secure Server CA	6C69E201656440EB98CD0875764A1ED19015ED8C4427601ACA9C68AFA8973959
Adobe Analytics - DigiCert CA	D5C009312F845C5EC8506EAD560D62447BFF4A60A9C25210511217AD6DE76AED

Subject Common Name	SHA-256 Hash
Aetna Inc. Secure CA2	5D28761CBF304EAFCD127B34D614FE179AC7744F1552AF1C31298425AD05A275
Aetna Inc. Secure EV CA	0A163600631BD66267FB7AEAD25C538B2B7D72AD6416A2BBD285F654BB642F6D
Aetna Inc. Secure EV CA2	1DDFDDF883E3945B2CB24FA5B83788379C5AB058422AB979DF66C77473988687
Alaska eHealth Network CA	437859303D0183862A96F6ABF8B03F2A69D4CBD317217666015E1ABA3C84AA11
Allina Health Connect HIE Intermediate CA	826C6AA610EF190BE2D7C03E22D032405B289804E3319E233C4C37FFBF305F1A
Amazon Server CA 1B	4A1FF6BBF481170D3B773CEC1F3A84DE3B5096575CDBF8B08432209318CA0FBD
Amazon Server CA 1B	F55F9FFCB83C73453261601C7E044DB15A0F034B93C05830F28635EF889CF670
Axesson Direct CA	BF4655F16AA338D7C7FF2BDC949A524BD4797B8B3C8341C608C9F65CB1CB8177
Cal INDEX CA	A5226F33474B53392665298B48F4E6129824E98BD4D38DF4E31EBBCF14FA33CD
Care360 Direct Intermediate CA	2D602B1F166D6316DAFD46B4B1EDD6DCFC54D2AF8A944BE358858FD504AAA16B
Catholic Health Initiatives CA	151A3591B765D02C359EEC9C56ED8DDAD0C54E756A497D02BF979FA8DD5D95BB
Cerner Corporation Direct Intermediate CA	09DE7FA739EE47C06291845F2E0E8A9E1C7CC2900AD354CF167316E02386BD9B
Cerner Corporation Resonance Intermediate CA	64284AA5F8DC8697D43D9737CF4E266625414E449C019667714537FF7EDE31B7
Cisco Meraki CA	199EE58009555DAE2CDA0626931C64391D6A88CCCB1F9F0B2EE80B667F581C06
CloudFlare Inc ECC CA-2	6172D7A1996CBEF71A0182DD44B99E9C035742A9EBD0311AA73AA4733344C5A6
CloudFlare Inc RSA CA-1	328C5991D8383E27D0EBE910BF66C0AF3D748A85D3011A52D88F1D8C8635647F
CompuGroup Medical Certificate Authority	B604026A3590392ABEFB6B18E8176453656115D2A0060F713E191A9FD076532A
Corepoint Direct Intermediate CA	CD2640957CF88610470CEFD409D85D9BE05962F7D6C2999C4F431ABCCC34118C
Cybertrust Japan ECC EV CA	92E3770B1EB44F84C2F2CB0097C2FD7126BD212B41C2610E78DDFD8946761738
Cybertrust Japan Extended Validation Server CA	0E10BDDEE7512DBD79EBF0B4F48FEED7C83C2BD3DD81765565F4FF110B7BFA42
Cybertrust Japan Issuing CA-1	87942388D29A46C06FE1E56AAB791594D0FB2E8EABF124048F130EEA9BEDD3FD
Cybertrust Japan Secure Server CA	33D57359831F87754E6E755D6B5B56E7E71297DDDFEA1D6397086604280F6FFC
Cybertrust Japan Secure Server ECC CA	C3683F7D91754219DADA4E8DC30E4B18BD3928B53D3AB93D07384BC5871CE355
Data Management Intermediate Certificate Authority	54837EF7B5AC4AA23606A15EF30DE46E9BB7E23E60F6ED4F2612092B94EDC68F
DC Government SHA2 Assured ID Intermediate CA	FB1147E7AB97A29BB9C1140ABF3DE831F4C5F60D11B90FEC999A0816375D8457
DC Government SHA2 EV Intermediate CA	F12241EE34C03A608D34DBC0EA465E1BD1AA13091554F9D4D086253FF3CE83D4
DigiCert Accredited Direct Med CA	0E78434EC8AD6613562C8390D8B3306FC6087E0593C7D5AC2FAF9AD263879745
DigiCert Assured ID CA G2	93C381CB07B353A920C2A7BED6BEBF195C68279DD0527D37F20BDD0D99C330FA
DigiCert Assured ID CA G3	634FDF26C994E76A2918D9EFC4CAB9C6FCB344EF642A79C89192BCDA0ED52F4C
DigiCert Assured ID CA-1	425E72C87FF22855D9908B71AB4C64B0D2F248287097690C62FE733F631DE38F
DigiCert Assured ID CA-1	B8F44E4B1F8697DF54BB3D0F1E67596CE2FE9DABA85AF4E6F2A2E74396F8C56D
DigiCert Assured ID Intermediate CA (SHA2)	C2B4BBEF4A1A643F334ED0850F928876D2AE3AE3642B986014D68C673C04D081
DigiCert Assured ID TLS CA	D7737E5F2D3FFCA429902E9F388CFD6C5959CD35A0FC103CEE2F7E93D1C66A52
DigiCert Baltimore CA-1 G2	BF1CB0E213D8D3C70BAE89429FC16DE2C74F755963D1B9B488BD0260DBC91B9C
DigiCert Baltimore CA-2 G2	F9690880819F06CDCC0B2F224B207F2AF6003FB57339B8679A160FA95208D62D
DigiCert Baltimore EV CA	D46931E0182DD655EA0C16E6DD99F8E61AFFE401F734C6CA8EA0056A968EAF81

Subject Common Name	SHA-256 Hash
DigiCert Cloud Services CA-1	2F6889961A7CA7067E8BA103C2CF9B9A924F8CA293F11178E23A1978D2F133D3
DigiCert Direct Med CA	F8F2D1C4123AF932654A52FBDFA06A9DB7FC412F28DF7C6EE50C88C8FCB1795D
DigiCert Direct Non-Provider CA	1AEDDADDC1ED748543EAF5960DF96AD51E21A3164F30A0640CB0732365D39062
DigiCert ECC Extended Validation Server CA	FDC8986CFAC4F35F1ACD517E0F61B879882AE076E2BA80B77BD3F0FE5CEF8862
DigiCert ECC Secure Server CA	458446BA75D932E914F23C2B57B7D192EDDBC2181D958E1181AD5251747A1EE8
DigiCert EV Server CA G4	710024B37BD9F0E1537C18A4C20F9A31C4B485D1248C643F20B4C00F3716BA85
DigiCert Extended Validation CA G3	7C0912E5DE8478BB86E8EA46BA5AE65DC3870BCEFCBC2F46795EEECF648CFBE7
DigiCert Extended Validation Intermediate CA (SHA2)	802C2AD1D215E57CDC9010EA437ACE399B657194FBD40E3BB5E00B080E6496DF
DigiCert Federated Healthcare CA	54C3F501042CDCC09AE8143CB192BD5E5724C9C88A6AB395A94A1A7AFC26CE7C
DigiCert Federated ID CA-1	DD46F8FDAAF66D5B68AA251EA2B214EC07EF8E2732A1ABA3B8A824D09F0F48F3
DigiCert Federated ID L1 CA	CAB016C5EA32061BD065FE13A55A40FA61058B27B34A7F8D175F7101EE063E3B
DigiCert Federated ID L2 CA	91FDEB52D4265120B843B195D1B6CDB5CE61251865A45A3E920E610FDDA660D3
DigiCert Federated ID L3 CA	85760F77DB0FD0D93C21EE0364B8EAB09B82CF49B7849831038209B5B1081363
DigiCert Federated ID L4 CA	EFB2A3F37273D3589047919825EA5337E9B938A8C178B61C18C2B4270B9665AC
DigiCert Federated ID US L3 CA	EB84FC0B403D9B689297A5D83EA186838E3B777BC618EFDA162A75B7FEA666C1
DigiCert Federated ID US L4 CA	6797436214EFEE67CDE7D70358D4D8B00DFBF78D5C87C62B4A7E790D73DD7BD9
DigiCert Federated Trust CA	E5BBDCCAD572EC9D2DD96E0E5EBF049A9181F070F1E33CC1635AD8EC487D2177
DigiCert Global CA G2	8FAC576439C9FD3EF153B51F9EDD0D381B5DF7B87559CEBECA04297DD44A639B
DigiCert Global CA G3	F7541CF69D1DE1AC953ABC1FAD6F7807A34EDFE9E12C11E66A195930C23AD6C6
DigiCert Global CA-1	3C750409882486D64151F4CBB5BD61432A4A7BF42F48A85198D245A64AEA2117
DigiCert Governmental Direct CA	5F665CBACC1E37171EA83EA85C570F9861CAF77BAC8886ABC4BB19B3698C094A
DigiCert Grid Trust CA	1E0A3AB993157717281D42ABF801EB64DEED500E4168CA706D6A71D8103C73A2
DigiCert Grid Trust CA G2	28CBB4E0D9C4EE6D04AC8F14717605AE3A4BD8CBF8D081B27AF6EDB2F3D76A32
DigiCert High Assurance CA-3	21EB37AB4CF6EF8965EC1766409CA76B8B2E03F2D1A388DF734208E86DEEE679
DigiCert High Assurance CA-3	57D8D5B832616B7823466A0C372770D16A5DCF246581F0F58373E51C7E1E5316
DigiCert High Assurance CA-3	C0A4A1AC05E03096A3B2AB8A38502B39E2614E11397BEE73D0A66B8ACEF7A283
DigiCert High Assurance CA-3	DCB400ACC249FB8483415FC2650BC90488CA96643118CB0E4F4424B21C3AA5A4
DigiCert High Assurance EV CA-1	4C4943B9EAA14EA2A69B8A7E4D8DA89081EEA11C87E8229B9B74F68A7AD33B79
DigiCert High Assurance EV CA-1	541AF019961760EF19E8FB4134E6D43085B5E5E087F30197DC42B2097E10487E
DigiCert High Assurance EV CA-1	8FC1469B8005BFEBDBF67F514E795FE1F17EA239A2A6934857F2428ADCE6D24F
DigiCert High Assurance EV CA-2	1188F831C949A62E9CD4F60E36F72544F0AF924DE07F9DA992E26E44C996EEE0
DigiCert High Assurance Intermediate CA (SHA2)	47511629F2BC3B7CF84EFEC9F32798A43AF6252E550B6CAE76A38558712E37D8
DigiCert Provisional Direct Med CA	C61029C8EEE3CE08755D562BB50C5F75E0EF849214970B13BD99185367D1D119
DigiCert Secure Auth CA	24E9F20AC167BB8F09DE8A1E9968CC53F0B5F3A4948F51B8647B40B186C75EBE
DigiCert Secure Server CA	94D4ECE2ED9A5457B969A13B260489E9A5FE4790A041F27A3EB4126C84418EF9
DigiCert SHA2 Assured ID CA	A542BCA09C5E4579C619774AE59082BCE0F86D261C5A7A5A0F6217C10279EA7C
DigiCert SHA2 Extended Validation Server CA	403E062A2653059113285BAF80A0D4AE422C848C9F78FAD01FC94BC5B87FEF1A
DigiCert SHA2 High Assurance Server CA	19400BE5B7A31FB733917700789D2F0A2471C0C9D506C0E504C06C16D7CB17C0

Subject Common Name	SHA-256 Hash
DigiCert SHA-2 RADIUS CA	524CF7331C4EE353EEB1ECD74E1F801A0F1F08DFA0322092F42205AFC3A17675
DigiCert SHA2 Secure Server CA	154C433C491929C5EF686E838E323664A00E6A0D822CCC958FB4DAB03E49A08F
DigiCert Trusted Server CA G4	6E8D952FDBABAD8DE3D61E094393739B5A47371A52BDCB2A3C2F8C43622F640F
Florida HIE Exchange CA	6FF1FE0046E7AEE94A181916C614682AE4FE6304E21821A05B149944EDA257D0
Florida HIE Exchange CA G2	AB8EE98A4B2B97E5905ECE80A64304C143AB38D9508FF7286F68235E0DB68A27
Google CA1	438F473EBFC8884EF5D3E0D52D264CDBE56CA382D9EBFC689D77489409F55A6E
Greenville Health System CA	06433FCA9F753980B526236DD72846EC1B20770BFCC7D3188DD67BC0ECFB7782
Highmark Tapestry HIE CA	1B68286DEFCE036512A5DAC76C8ABD067D33A07D4E0DEF7707089C980075E192
Huntsville Hospital System CA	20E3E88747A8D88E11A527521032DC8CAE92BC33B45C93EEE04F624A70DC920A
Indian Health Service-RPMS DIRECT Messaging CA	C07E9037CB81012D3046613285C14B63A0284964A4F5A821FC3B18ECDEBA0A66
Inland Empire Health Information Exchange	1E72D83ED9499CBA686968452BE591C48816EC9181391A5D03C1F4D3BA1658DC
Inpriva Direct Federated CA	5AE4F777426BBC5AA85986CA48D319270C5536210DC8EA1A28D502F6B3595138
Inpriva-ClickID CA	60C62B09AB92EF0E31DDA889E65BC9F0CFC98E6E369A3AEAB0EE0E2AED855581
INTEGRIS Direct Intermediate CA	97D276C5FDF2DC94539ABB9E17BC3995730CD51739EAE95B0F67B39E99905F11
iShare Medical Direct Intermediate CA	4C0A5888C34AA01B745F4EBA268696B2CCB3F4AA31C8EDCB3AFE8FA84CB74CC1
Jax HR Saint Vincents HIE CA	3D2928A2988227CE4EBC319AA34E6552E9D98839D5CE2114E79F8F5EC2BF9DE0
KeystoneHIE KeyHIE CA	D1C2009D472835AFBA94CC8ACB06DD0C727138AE1E73834394D27B0C06CF1265
Louisiana Health Care Quality Forum CA	3E4F09D65438B5CF7E456288C08FE9F47ED4E3ED669279C81AEFAB0BAFB86A09
Mary Washington Healthcare CA	1180C33AE1F23228923F6AE698C9C10DC729E0D811FC8B2EC02726E2DC26E2E4
Mass HIway CA	23BA3A97C580DF2C316624D7FA5F7663580261CB2048142C73A3E86B113EB26D
MedicaSoft Direct Intermediate CA	51A6E2ED41040AAE8E089FBABFE26A38D656F5B0855635352FEE9598286BB021
Medicity Direct CA	231BA402E28B3495F3BE0CAD87078D9B8FBD86041116AF9B8047E7B1CFFA82D0
MHIN Direct CA	EAEEFB08D568E7F6CF6D892CAB6A22E14F20C6F10E3A418CFB42B12309333367
Mirth Direct Intermediate CA	CC9FAAD83C3350943D4E45FA416C4F8BC564F7AA94CF4B2D2BCE74209D0464C9
Mississippi Division of Medicaid CA	1757291A3D7D0BB5B9B9CF8802F1B2AE173E56B0935970FC86B63A27499DB5E2
MobileMD Direct Intermediate CA	33CF1F5C9396D7EE9E8283B2E76F400E50450575EB15AD02C956C1C5575B184D
MRO Direct Intermediate CA	E25DE970AA8B685CDF55417897F65DE64C63A55D61EE9E4B830261DCFBBFFFB4
NCC Group Secure Server CA G2	6075DA5CECD15D6584C5560322D5C09FC2199E52DEA7921D91040AA75248672E
NCC Group Secure Server CA G3	963056B0D941D9DBE27AC778053D85E43CC79F476AD34CFDD799C27E381840EB
NCC Group Secure Server CA G4	B7DFDC27E5FF9F35EFEC9F4BC532C35F727789B69C90A0489B40247299D97038
New Hampshire Health Information Organization CA	37E9A271EB4725C93CDAF183562C7D7D9EA8FC139F8374FFE418D77D32428FE0
New Mexico Health Information Collaborative CA	10BEDDC480AA27563480B1BCAAB6C25B52995EA836E9A2ACE83F8F59206E2496
North Carolina Health Information Exchange CA	C4A842434ADB52809526B6D1E869A265F535B69BB16454A301667CC942678D58
North Dakota Information Technology Department CA	6ECF658CCEA8B29BE60C85904F4ADD7CCB7950CF58C97BBF60D57CEA49A2703D
Oklahoma State Department of Health CA	77ABE65DF4BE94E5EC222FC905E1233F8C77D6B3AE2933346A0C2FC3B2F1F560
Optioncare CA	89CFBC8FBFF7FE026B6CF2EA688419BDE8BBC1FB451329C865D6C6CBCF6BD097

Subject Common Name	SHA-256 Hash
Optum Public Trust CA 1	253E3C9732DF8874C3D54DA522C1711142C98C2CEA7664635152A89A03EE9364
Oregon Health Authority Direct CA	86FFEA40F36FA6913278710FEABA9B206F3288DA3FD1C652BC5B5895A2B1A877
Orion Health Direct Secure Messaging CA	A4106DA85F7B34A6D3DE37884D1528916B84F046FFB7D4AAC521117B0C6995F3
Orion Health Direct Secure Messaging Public HISP CA	D34138ED1458AE7DE4EDEA36ED3992E4F46E6EC9CF1E633E538DE9FF0F38F8E5
Plex Devices High Assurance CA	48A7C9C5A36734FC9E204D63CE6BBBCD9E21C1978604760CD8D30D6F4C67B67C
Plex Devices High Assurance CA2	50D3D71FC0CD7E36ADAE32221FEFBE8CC29B2676BA326C09B8FA1B24DBE75514
Postecom CS4	C1685683F3C8590E88580197F219CAB99E5482A1568635F596D09867B2F405BD
RelayHealth Direct CA	77537682E9A0B2C5BD5E62BC1CB35ECEB38FCBEBF7D2DC326F7E420F0DDBEDB3
RITC-Inpriva-ClickID CA	3124EC8537998F02AA431F0EA9D34A44ADD358A23681657149143C6607DE48A0
Rochester RHIO Intermediate CA	43202B9E870659921F9DA26EDA9E47BF6990DB031A0BC0B23AFA1E7968ED3E99
Rush Health CA	DB12B1D3F8CC52FFF4874F0A8B85E9FB6A2050861B1B1C61481A743AC0D33D5A
SCHIEx Direct CA	443C8158264710C0B768A8170E59BF1FAE4079D2BC39939A79FA839174ED81AE
Secure Site CA	D3533B732A518A6DA68EF266085E11DFD114C0EB0092CD43530A44D54B913ED1
SecurityMetrics DigiCert CA	F32DEAF22CE724661F53D5287311AFF2541EB38ECAF49DD877B94023E3A11B1F
SecurityMetrics DigiCert EV CA	6B2328E7FFF598B2ADF90B7F3EA42B45FA606D78E2B117B7D60E99E828CF7565
Sonavation IoT CA	4C56CA7A3C10EB58765E0FFCF8035C57C9F3BDB014862F676756CF789193F10E
Sutter Health CA	603D69822381A0BFC274BBED67009BC7DF133CB902FA242CF58BF727D23D5495
TERENA eScience Personal CA 3	FDA947208BFA3203A6C57B8714A647B7009E5168E88951345450B1D2D3F91A7D
TERENA eScience SSL CA 3	E1BE6BBBB70F5A241E736FC44C6A2160BF6CE19B95EDD67BF7BE896E83778745
TERENA Personal CA 3	DD4E0C17900F3FC2A5B7B773AE40218AD73216B5CE5D285EBFFCE8830D0F034A
TERENA Personal CA 3 G3	C123F5AFACC9F9096809850355E5BF78CA9377348111B5167A964DDEDC044DE9
TERENA SSL CA 3	BEB8EFE9B1A73C841B375A90E5FFF8048848E3A2AF66F6C4DD7B938D6FE8C5D8
TERENA SSL CA 3 G3	C9D6913F3FEDDEFF184C9EE1D7E17C5AEC90886EED5CC3D6E98105831C8C0E0B
TERENA SSL High Assurance CA 3	BE6A0D9E1D115F2293F6ABF11B3EC8E882E24426EEEB09AAA503597993E77A25
The Koble Group CA	A576C29481F5A2ACB1DF47500629A60F96F6ACA324E878FFDCFABD85E5649AEF
Trust Technologies Global CA	191E0B48B78B7EFA4822A465AD69B34405B878D10BD853D8E57CB8B9D9E50B8B
Western Connecticut Health Network CA	415322F3970C8CD0F54311E0F93C5F5C37BA3059FDB10F5240AC20934717F840
WoSign EV SSL Pro CA	891EE2E23282E5076C9AE9047DE8EA900E066F81D6DCD9B843C59078B0F105BC
WoSign OV SSL Pro CA	AA61C2927DC89DB225CA9A17D600373D058F696D86D10E2BD7B5E8F44A97EED1
WoTrus EV SSL Pro CA	070531383CCD100D3E9CD964DB07AA5E845A0686F2EAE3BC8A627B182057B1F1
WoTrus OV SSL Pro CA	09033FE23996FE4A59C4C0F523D2560E31DFE4C17D8EA1403D429A971F4BD65A