Ernst & Young LLP
1775 Tysons Blvd
McLean, VA 22102

Tel: +1 703 747 1000
Fax: +1 703 747 0100
ey.com

Report of Independent Accountants

To the Management of QuoVadis Limited

We have examined the accompanying assertion made by the management of QuoVadis Limited (QuoVadis), titled **Management's Assertion Regarding the Effectiveness of Its Controls Over its Certification Authority Operations Based on the WebTrust Principles and Criteria for Certification Authorities v2.1** that provides its Certification Authority (CA) services at Bermuda; the Netherlands; Switzerland; the United Kingdom; Belgium and Germany, for the Root CAs and Subordinate CAs referenced in Appendix A during the period from 1 January 2019 through 31 December 2019, QuoVadis has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certificate Practice Statement, and Certificate Policy:
  - for the QuoVadis Root CA, QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3, in the QuoVadis Root Certification Authority Root CA 3 Certificate Policy/ Certification Practice Statement, version 4.28 dated 23 August 2019; and
  - for the QuoVadis Root CA 2, QuoVadis Root CA 2 G3, in the QuoVadis Root CA 2 Certification Policy/ Certification Practice Statement, version 2.7 dated 20 June 2019.
- Maintained effective controls to provide reasonable assurance that:
  - QuoVadis' Certificate Practice Statement is consistent with its Certificate Policy; and
  - QuoVadis provides its services in accordance with its Certificate Policy and Certificate Practice Statement,
- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - The integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - Subscriber information is properly authenticated (for the registration activities performed by QuoVadis); and
  - Subordinate CA certificate requests are accurate, authenticated, and approved,
- 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 management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the Chartered Professional Accountants of Canada ("CPA Canada")'s WebTrust Services Principles and Criteria for Certification Authorities Version 2.1 (Criteria).

Building a better working world

QuoVadis' management is responsible for its assertion and for specifying the aforementioned Criteria. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our 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, which includes: (1) obtaining an understanding of QuoVadis' key and certificate life cycle management business practices, policies, processes and controls, and its suitability of the design and implementation of the controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems integrity as we considered necessary in the circumstances; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, 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.

QuoVadis Management has disclosed to us the attached comments (Appendix B) that have been posted publicly in the online forums of the CA/Browser Forum, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these comments in determining the nature, timing and extent of our procedures.

The relative effectiveness and significance of specific controls at QuoVadis 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. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Our examination was not conducted for the purpose of evaluating QuoVadis' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, QuoVadis may achieve reasonable, but not absolute assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are achieved. 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.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the

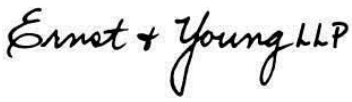
Building a better working world

degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

In our opinion, QuoVadis management's assertion referred to above, is fairly stated, in all material respects, based on the aforementioned criteria.

The WebTrust seal of assurance for Certification Authority on QuoVadis' website 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.

This report does not include any representation as to the quality of QuoVadis' CA services beyond those covered by the WebTrust Services Principles and Criteria for Certification Authorities Version 2.1 criteria, or the suitability of any of QuoVadis' services for any customer's intended purpose.



Ernst & Young LLP

31 March 2020

Management's Assertion Regarding the Effectiveness of Its Controls Over its Certification Authority Operations Based on the WebTrust Principles and Criteria for Certification Authorities v2.1

31 March 2020

We, as management of QuoVadis Limited are responsible for operating a Certification Authority (CA) at Bermuda, the Netherlands, Switzerland, the United Kingdom, Belgium and Germany for the Root CAs and Subordinate CAs listed in the Appendix A. QuoVadis, CA services provide the following certification authority services:

- Subscriber Key Management Services
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Status Information Processing

Management of QuoVadis is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in QuoVadis' Certificate Practice Statement, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, 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 QuoVadis' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of QuoVadis has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in QuoVadis management's opinion, in providing its CA services for the Root CA(s) and Subordinate CA(s) listed in Appendix A at Bermuda, the Netherlands, Switzerland, the United Kingdom, Belgium and Germany, during the period from 1 January 2019 through 31 December 2019, QuoVadis has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices as below:
    - for the QuoVadis Root CA, QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3, in the QuoVadis Root Certification Authority Root CA 3 Certificate Policy/ Certification Practice Statement, version 4.28 dated 23 August 2019; and
    - for the QuoVadis Root CA 2, QuoVadis Root CA 2 G3, in the QuoVadis Root CA 2 Certification Policy/ Certification Practice Statement, version 2.7 dated 20 June 2019.
- Maintained effective controls to provide reasonable assurance that:
    - QuoVadis' Certificate Practice Statement is consistent with its Certificate Policy; and
    - QuoVadis provides its services in accordance with its Certificate Policy and Certificate Practice Statement,
- Maintained effective controls to provide reasonable assurance that:

  - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - The integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
  - Subscriber information was properly authenticated (for the registration activities performed by QuoVadis); and
  - Subordinate CA certificate requests were accurate, authenticated, and approved,

- 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 management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the QuoVadis Root CA, QuoVadis Root CA 1 G3, QuoVadis Root CA 2, QuoVadis Root CA 2 G3, QuoVadis Root CA 3, QuoVadis Root CA 3 G3, and the issuing CAs listed in Appendix A in accordance with the WebTrust Services Principles and Criteria for Certification Authorities Version 2.1, including the following:

CA Business Practices Disclosure
- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management
- Certificate Policy Statement
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Life Cycle Management Controls
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

Very truly yours,

Anthony Nagel
Director
QuoVadis Limited

Appendix A to Assertion of Management

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis Root Certification Authority OU = Root Certification Authority O = QuoVadis Limited C = BM	3ab6508b	A45EDE3BBBF09C8AE15C72EFC07268D693A21C996FD51E67CA079460FD6D8873
CN = QuoVadis Root CA 1 G3 O = QuoVadis Limited C = BM	78585f2ead2c194be3370735341328b596d46593	8A866FD1B276B57E578E921C65828A2BED58E9F2F288054134B7F1F4BFC9CC74
CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM	509	85A0DD7DD720ADB7FF05F83D542B209DC7FF4528F7D677B18389FEA5E5C49E86
CN = QuoVadis Root CA 2 G3 O = QuoVadis Limited C = BM	445734245b81899b35f2ceb82b3b5ba726f07528	8FE4FB0AF93A4D0D67DB0BEBB23E37C71BF325DCBCDD240EA04DAF58B47E1840
CN = QuoVadis Root CA 3 O = QuoVadis Limited C = BM	05c6	18F1FC7F205DF8ADDDEB7FE007DD57E3AF375A9C4D8D73546BF4F1FED1E18D35
CN = QuoVadis Root CA 3 G3 O = QuoVadis Limited C = BM	2ef59b0228a7db7affd5a3a9eebd03a0cf126a1d	88EF81DE202EB018452E43F864725CEA5FBD1FC2D9D205730709C5D8B8690F46
CN = Bayerische SSL-CA-2016- 01 O = Freistaat Bayern S = Bayern C = DE	6c508d1fb1e365278309f895997fe98b6ee1853a	D852DE5D098086DFE9A6F3D728D5261865587C489DE675753D272374A5D6E9FC
CN = Bayerische SSL-CA-2016- 01 O = Freistaat Bayern S = Bayern C = DE	074d7e05edf8885cdacb24f039fa40629aadfff8	E8CA72ECB9885C24EA29DE0EAC97704278D2A1E59B66666D327FB0CC6BDD912F

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = Bayerische SSL-CA-2016- 01 O = Freistaat Bayern S = Bayern C = DE	169b62744e8c7c77388baa8bd8f10ad414212d26	4874758D6563E0433B1EDCEE7CCC5D9C2AAD8EBA12BCB0704454BB4EF8EAF799
CN = Bayerische SSL-CA-2016- 02 O = Freistaat Bayern S = Bayern C = DE	05f4a334090f7b1ae83677d4766bfd32a71e0851	806A2AA77EDBD3C76D8FD066DFB5CC3310F359B0102CE92C0FAEC16AA43FFF0A
CN = Bayerische SSL-CA-2016- 02 O = Freistaat Bayern S = Bayern C = DE	45a93afd305dfeb3cd0531dc0e329cf42a4e99d3	33CD537E009DB9C758A568435C06706F9F01138054E20B9DDC93E0397138AA6B
CN = Bayerische SSL-CA-2016- 02 O = Freistaat Bayern S = Bayern C = DE	301afac8acb6d1ab342eb39e684bd912d9f1ddce	FF1DD21F1A5D0B452CD969CF4AA553835CABE0293C6C7B009F145AA202C02C8B
CN = Bayerische SSL-CA-2017- 01 O = Freistaat Bayern S = Bayern C = DE	15722c4538cde50e6cbf4f48f521c25bec9b5a5e	3BF1E41503C7F023D0D4CAFFBE8E51262C2C7310BC6D96E8CC8D143A600AEE80
CN = Bayerische SSL-CA-2017- 01 O = Freistaat Bayern S = Bayern C = DE	055bdf5cae52faa69f1e167af9e466a114e177ab	B39627401441CEB42FF6C7F983E0F2A9230D1877403C9F40965C8757CEBFD7D6
CN = Bayerische SSL-CA-2017- 01 O = Freistaat Bayern S = Bayern C = DE	6eb571b1aee67f603cdc59fe8b638dd6c6e88e36	8D9CFD98F52B1C2C6F4E9CED3D1D995927EFB0D5638FBDF08834D0F72CA29118

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = Bayerische SSL-CA-2017- 02 O = Freistaat Bayern S = Bayern C = DE	107820596210c5bfc0092ce2abca189079766e06	0AB115DE9D126A3D4EA10DDF0863CC9D8956744EB7B4CCDAB7E57D6A06E58518
CN = Bayerische SSL-CA-2017- 02 O = Freistaat Bayern S = Bayern C = DE	4823e5da20b8401683cc5d7dc21d3520dd690bc1	7B85F6D0859B240A3363374A1181E012021047DCED2352A841F6E55B5D077EA5
CN = Bayerische SSL-CA-2017- 02 O = Freistaat Bayern S = Bayern C = DE	78105ef8412c61f3b91d09275705bebf510a29dd	425202D4BBFDA9B799D0F7AA927D944F42CCA4237C2FC19875B9075DEB35A621
CN = BEKB - BCBE Issuing CA G2 OU = Issuing Certification Authority O = Berner Kantonalbank AG C = CH	289fbf1348498bc26512ff3abf8af52f2a0b7502	B399EFE42C01A05BDC38978447A78E950467793FB11C1B6B426C419A0FC73911
CN = FMH CA G1 O = FMH Verbindung der Schweizer Ärztinnen und Ärzte C = CH	463f93870b0003c0eaa102d749aaaa125c8af4fe	A0AF1418CD14F6B2415EC6316C7D588BB25D430A3D6D026F57DE20F965EABDDC
CN = FMH CA G2 O = FMH Verbindung der Schweizer Ärztinnen und Ärzte C = CH	7d2c2572d198339c0e67a4ba49ba5f690a0b094c	B968FBFC3ECA285AADC38D2367727241FF7D3733F1278F8A4F50ECC8C0EF1E80

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = HIN Health Info Net CA G2 O = Health Info Net AG 2.5.4.97 = NTRCH-CHE-103.489.218 C = CH	35bb9264f660c9bd09f8c0b34617dc2b1341e05c	3645E0F05E195BE8ECD456E518C8C23C1BB259CD6CF4691F29C744AEF0C11FDD
CN = HIN Health Info Net CA O = Health Info Net AG C = CH	0a29	479F4E101F380691201A34CBADBC09E5F0523B35EE3839EB4B14332481EF8463
CN = HydrantID Client ICA O = HydrantID (Avalanche Cloud Corporation) C = US	5654d76a669eeeb418daf62cc1196b39b480e899	2EEE91CC892A16CCB7320CDED2AE4948C052345D6B24E214C24EB93932D10DD9
CN = HydrantID EV SSL ICA G1 O = HydrantID (Avalanche Cloud Corporation) C = US	5bfdd1bb152d106baa6d6d17e73c561f0dd9c8ca	80FDE428212AF0CA0AC531EEE6ED2DF3D3C2A4557DFCE857070FC947922E9B24
CN = HydrantID SSL ICA G2 O = HydrantID (Avalanche Cloud Corporation) C = US	7517167783d0437eb556c357946e4563b8ebd3ac	9C6D08933201407FBF2B12540B67CC0E4C9666F132E1504762A717CBAE8F3FD6
CN = QuoVadis Belgium Issuing CA G1 O = QuoVadis Trustlink BVBA C = BE	6acaf5c985274c5027ba29283006d6e4c4f15a9b	27EBACD86DD3BF86143DA4342861031A57CF3FA414D40A86E669C3F4F1D8CF24
CN = QuoVadis Belgium Issuing CA G2 O = QuoVadis Trustlink BVBA 2.5.4.97 = NTRBE-0537698318 C = BE	40f6065343c04cb671e9c8250e90ebd58dd86e55	D90B40132306D1094608B1B9A2F6A9E23B45FE121FEF514A1C9DF70A815AD95C
CN = QuoVadis Code Signing CA G1 O = QuoVadis Limited C = BM	1ce6507ec1d9c0b16178feee058cae7a0b142858	DA0AFAF15CD300E34B520FB78A4FA68EB42C4601E939B903E0B1D71DF5965BFF

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis ElDI-V CA G1 OU = Issuing Certification Authority O = QuoVadis Trustlink Switzerland Ltd. C = CH	1387500c423dd8187e315b36686765216f2b9035	393E95D3AE5233A04FEFE058BA8F445132D30E4362D5F7259061392716B34D2C
CN = QuoVadis Enterprise Trust CA 1 G3 O = QuoVadis Limited C = BM	0ad86fa335b93ef48c8e3bf77d4c63143643adb9	0531C86F785958939FDC539924D395D1EFA409364E6827D3AB9876311FFB27B0
CN = QuoVadis Enterprise Trust CA 2 G3 O = QuoVadis Limited C = BM	5eeeb44a70e18e63c9898f202cbac164914edc05	174E1DE77C8D93C68ECD2BD2EA6E191B584DB850277A834AAC898B7C80A91C70
CN = QuoVadis Enterprise Trust CA 3 G3 O = QuoVadis Limited C = BM	0c2163a44924ffb7fcdb675acdcaee7208cca95a	DA5462526A0C2E9852A86186B025390158759CDCA6AE21F09F713CA6ACCDD1F1
CN = QuoVadis EU Issuing Certification Authority G2 OU = Issuing Certification Authority O = QuoVadis Trustlink B.V. C = NL	2018702e0e3f979bdc163037d03bb6d27d5c4b22	EC3F940A48EF7CBCEA4142F735A5DF2976DB38183D9033C76B78E25F8F53EB5B
CN = QuoVadis EU Issuing Certification Authority G3 O = QuoVadis Trustlink B.V. C = NL	375b8adb585dd26543ec430b8700530c7e10fd9e	ADDFFA6FD0809A54A9F0B31FD25F74BF7F2D7AE11C80FD99DAA0FB603A65CD0E
CN = QuoVadis EU Issuing Certification Authority G4 O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	1588bb1a8ab4171349888c596f21e39f1e18ce3e	0DD818228990D83FCE9F9DCA7B5CC44ED318EDD16399987EA893877EA52DE11E

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis EU Issuing Certification Authority OU = Issuing Certification Authority O = QuoVadis Limited, Bermuda C = NL	421fd4ce	EC50E7E17D3802811C8B6567148CED68BBB1BD79EDDC61DBD298CEA5BA0FB862
CN = QuoVadis Europe SSL CA G1 O = QuoVadis Trustlink BVBA C = BE	4db89836333b16bc441d5f4fc60bc67dcff0bd28	DC8B2DEE50DD478AB135CAC269CEA68851557A9129ABCD98DF5213B23DBFB3CD
CN = QuoVadis EV SSL ICA G1 O = QuoVadis Limited C = BM	73da5afa23d93fba842e0a20f401c9d86e24fc5d	3FE8BE392A08684B99F497E618C7DDF5A02A4289BF9D08E595045931BFBA814F
CN = QuoVadis EV SSL ICA G3 O = QuoVadis Limited C = BM	524fc1f16e34d1702b84a13fb042bbcc7c3c9032	F18442BEDF70B4D15211356C72B659332BED03FFD3BBA7AFAAABE6DE9D723002
CN = QuoVadis Global SSL ICA G2 O = QuoVadis Limited C = BM	48982de2a92cb339e1c8f933358275d3e4f88255	A4879EC0F36CF84B6F2ED87AE57EE3B94A0785C6862238CD45481084D152EB18
CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM	7ed6e79cc9ad81c4c8193ef95d4428770e341317	CAB9C12DBDE3AD5D2BC0201B54B18BE209CD5E146AAA085ABBDF241B096DFF47
CN = QuoVadis Grid ICA G2 O = QuoVadis Limited C = BM	10b62f345a61eb6184a7b106c8057e9453e207d5	74CE8C1631EF9F38E7A4197DA3F5474DBC34F001F2967C25B5999562BCC8C9D4
CN = QuoVadis Grid ICA OU = Issuing Certification Authority O = QuoVadis Limited C = BM	421fd45f	53007E9E70DC1FFF21FC813649F5DAF5FCE3A244DE6B43D691B10DDA262DC0B7

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis Internal CA G1 O = QuoVadis Limited C = BM	6e3e67e28cd49bf0011c75679c15c72d3804d1de	6B8973A0DBADA29988C5DC06CBCEF049BE770604F8A7436D817FAC3A9710F481
CN = QuoVadis Issuing CA 3 G3 O = QuoVadis Limited C = BM	1d9c5b8a40a58a16fed4f336724d120c467cfdd2	C12DD0347C0D4AA25D3986E0499740C5363A6B7EC32A49C5D18B9D56B075E368
CN = QuoVadis Issuing CA G3 OU = Issuing Certification Authority O = QuoVadis Limited C = BM	421fd5b3	15CE38976716DCB35AA7B35FC168EBBB3BC2EC4696A8C795FC5C48457140E0A7
CN = QuoVadis Issuing CA G4 O = QuoVadis Limited C = BM	69b2d1ccf02e20dcc95c62894f7f9e5f5fc057bf	DA3BC81005FDBB853D681A7E942661AEBA23789211525EAF52221F28514C09CB
CN = QuoVadis Personal Signing Service CA G1 O = QuoVadis Trustlink Switzerland Ltd. C = CH	689db6c7841e4b5b09a8184ef3fd79193b118247	F94C931373F850FF3D7DB5FB20AC04EC2F812CAEC9BD17E32DB6DCAE2269104D
CN = QuoVadis Qualified Web ICA G1 O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	4984b32ba495d0c61de34bcf14d3a35aee508644	C02D8A30ED69B2F864ED8FB1A63A3E7255288920CA294BDCA30F63898FB9195C
CN = QuoVadis QVRCA1G1 SSL ICA O = QuoVadis Limited C = BM	760bdb66c0c72c1590385851c8835f226dbcf063	9058D5065F8F3E9A63AAFE5CE89A764470B0DEF9DCF3B9EC7D0587FAB88FEBA0
CN = QuoVadis QVRCA1G3 SSL ICA O = QuoVadis Limited C = BM	749e30fc6c0fd3c59e91b5085ef613b10acef9af	51587C867BF66F35ECE554A08E0A41C13B8BBD9B59D262D204A70309A672BEE6

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis QVRCA3G1 SSL ICA O = QuoVadis Limited C = BM	1af6d97a8ff0b28deeac01a524c87a6f32e79df6	8D99217FF82D60E4DF59BE8A1121625CDFFC4F22F21E1263A1DF06D2DC0B540E
CN = QuoVadis QVRCA3G3 SSL ICA O = QuoVadis Limited C = BM	454304f0e63f6011f2a246e0c684caa4f7288876	764A0D84D5552CD5872C73464F37F02175CDA70588102B13ADA2A0199FC403E9
CN = QuoVadis SuisseID Advanced CA OU = Issuing Certification Authority O = QuoVadis Trustlink Switzerland Ltd. C = CH	421fd595	5DDAB0A802D83893AC0EDF9B30A620411B1A74A8B7D411A6A7AD7DC46EB1C8C8
CN = QuoVadis SuisseID Qualified CA OU = Issuing Certification Authority O = QuoVadis Trustlink Switzerland Ltd. C = CH	421fd596	5B7017B80F97C621AF1163B04BEBAFD2F932A42B85F4B9FEC71B38609F564922
CN = QuoVadis Swiss Advanced CA G2 O = QuoVadis Trustlink Switzerland Ltd. C = CH	6a280af346232831c95b42c29d24c4a82cc335e3	5044F65E1042CD380B0B9997E4283358F0DEEF7873DA72EFDB6F02474AE37EBE
CN = QuoVadis Swiss Advanced CA OU = Issuing Certification Authority O = QuoVadis Trustlink Switzerland Ltd. C = CH	421fd59f	235C96A2E2DA557B904E90F3A0CAA57EABB4BDB5F401969DA8C282F60839568F

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis Swiss Regulated CA G1 O = QuoVadis Trustlink Schweiz AG 2.5.4.97 = NTRCH-CHE-112.210.349 C = CH	3b0c1728097a64faa02d851b9affb5705e60ec75	53570D05E40DC62F9DF91D15AFB015B56AAA680C20CC168E6D57D946C9CE2684
CN = Allscripts Public Issuing CA 1 O = Allscripts Healthcare LLC. C = US	098eb7f54f6c9f4b17d7c741e3856495b29eb1d9	5BD0C0D579801567F3388FE644EF790AB31E2DB2246EAF4C881E5A57D9A0A582
CN = Bayerische SSL-CA-2018- 01 O = Freistaat Bayern S = Bayern C = DE	44915f9e749ae3af4f9b67f6ff1c82b45f444bbf	52B63D1BD08E83BDC723D7B1FE962CEC1806E7F53F76F2C70858CA35293A1DC1
CN = Bayerische SSL-CA-2018- 01 O = Freistaat Bayern S = Bayern C = DE	22559aace2195a18cf8e404896b94132a8dc4ccf	C84AE01ECD202DAFBEEE1F0E679646DE8CCD653D7846718A3B5F4E129324298A
CN = Bayerische SSL-CA-2018- 01 O = Freistaat Bayern S = Bayern C = DE	5dced5064c9e3513c0524ad49972fbc5d37e7713	0F751035C18E1D392E9CC557C57E94A55D12FBB086F26A4529E2613625BFD13C
CN = itsme Sign Issuing CA G1 O = QuoVadis Trustlink BVBA 2.5.4.97 = NTRBE-0537698318 C = BE	3b30442898d3be1cf55c5ea5ff04d6fb74701cd5	F640E5643C40C1F329E100438E28C957691AFA8A53E405A326F7AFEB70C23BC1

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = LLB Root CA public v3 O = Liechtensteinische Landesbank AG C = LI	703debe2413f067aaf7282b51bfe35c0b17e0148	FD4C2B993E0356E90D4F9FBD2361DEF1A498378CEECEB92DD76FE0AD7E2C7B16
CN = LLB Root CA public v4 O = Liechtensteinische Landesbank AG C = LI	0824c2739a3eb7a1d14f54b71b1390cfb7c27c3c	3A59C1A60A69FE57A98DAB376736275AF0913FD1F65B92B71B7E9A7A1EB440FE
CN = Novartis Issuing CA by QuoVadis 2.5.4.97 = NTRCH-CHE-106.052.527 O = Novartis Pharma AG C = CH	3c6c7abce6742e8c32716b2103b976fdc4bd9791	2C0971F397BA8737B033584556906594936ACE1753A5A4BE5E2F11B42BA4B759
CN = Novartis Issuing CA by QuoVadis 2.5.4.97 = NTRCH-CHE-106.052.527 O = Novartis Pharma AG C = CH	6caa4e8dc75aaddbd7542b2310e0aaa0fd7fcec1	8F4145BD48CC9BF722925923E7D2D09CCCBE9973A53838CA36F9561F74E8C271
CN = QuoVadis Europe Advanced CA G1 O = QuoVadis Trustlink Deutschland GmbH 2.5.4.97 = VATDE-DE296898382 C = DE	2332c55aee4085189ac0b6e83946ced64ba74e6a	8E5CEA1D1012521C27A4E11270702BC7C9A1156F135073D6CA4E42EEE826249E
CN = QuoVadis Swiss Advanced CA G3 O = QuoVadis Trustlink Schweiz AG 2.5.4.97 = NTRCH-CHE-112.210.349 C = CH	41e89ed3562149c894bddb7bdedd7ec569c72490	31A7C579F24D5562CDB203FA15A9F2C3FF5DC1F2E6BF7C0BD95FBCB0114C8D21

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis Time-Stamping Authority CA G1 O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	4335c24f7215311c1098838d7a0d5584cdbf517f	D2BA0BFEC43FA7803860CDE6B3377421B1F563EC124B51D908415B0E937323E6
CN = VR IDENT EV SSL CA 2018 OU = VR IDENT O = Fiducia & GAD IT AG C = DE	6fa3cc76e393d62826d9be57ad26cdd5ac91603d	BF39A4241F42D522368944B3DC53ED9EAA5AC7735E242E0627C0DD5BBA714484
CN = VR IDENT SSL CA 2018 OU = VR IDENT O = Fiducia & GAD IT AG C = DE	43a90e0f1875301023583e27e8fb80b9edc64b0e	502C7A870341D7BE67DB26DBFACF9647AFD89A854BF8812FA4EF70C356EC13E5
CN = QuoVadis EU Issuing Certification Authority G4 O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	127f8b32062628c0ca3f8d44bef9f2fa5db1440c	1D24222B5EEC71FE99BE9D700FA5FF72312DB3EB0FCB4A4F3BCC135DA36C1355
CN = QuoVadis EU Issuing Certification Authority G4 O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	6488b3ffd2c6bfb39d3bf05a9fc054500a8d7723	7F93E8E4BEE47624CED4E8384DBA96C4828D461D787D0AE3EB316DE985D51C6C
CN = QuoVadis Qualified Web ICA G1 O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	18917d9ba1a239a92a20d96d7d76d942dc4a1065	04ECBA8F92BFF7458C4A5E7C69261FC7E2EF52D5AF54FBDD92B17141BBE0651F
CN = BT Class 2 DigiCert PKI Platform CA O = British Telecommunications plc C = GB	72c987417647231d21a5a1e13234c80f33fc35a5	843782303040BFB33576766E1700696DE0FC14887BE293D7265EB59ECE4ED9CC

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis DC EU Issuing CA ECC G1 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	46f8044efe241e38c2d5dbc9062b119e09e9bc38	0978125AC198DB396B613CE053A6CFA32D22169398F10A8BD879C52F3E51D575
CN = QuoVadis DC EU Issuing CA RSA G1 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	765a70ee540807fd46e096afc27ee69da84d4c07	6745D87F4A374D8F02AE2DE9A353315275548CFFC6CE94C271B82BF7A63230FE
CN = QuoVadis DC Qualified Web ICA ECC G1 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	56ec68f1ead371bd2d3ef4a77bcbe6ee9a0019f8	BDE762813E825A2669D413F82CBA26DD8419B8A069939989FEED222FE67AE78C
CN = QuoVadis DC Qualified Web ICA RSA G1 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	24dec42507fc86eccbc448c7762b2b0ce82bd2c3	C522F888E49F77C232C26B0D35E746B689C470645A4AF431A652D84448F7A071
CN = QuoVadis DC Qualified Web ICA RSA G1 2.5.4.97 = NTRNL-30237459 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	0ca290f1b7180f09f83e8c2ce8a8735ba271318c	83EC6FE4DD64463AFE6F695B0AAD5F17655990B4D858EB80225F875A6B4F01E1
CN = QuoVadis Issuing CA G5 O = QuoVadis Limited C = BM	61be8292e7e8cb3adf98e2ca7af34154298dd068	08204C52ADDAA97A6FDEF702F6CEB4B94E578F8FC1C301C9D5136AB381CFA7D9

Distinguished name	Certificate Serial Number	SHA256 fingerprint
CN = QuoVadis Swiss Regulated CA G2 2.5.4.97 = NTRCH-CHE-112.210.349 O = QuoVadis Trustlink Schweiz AG C = CH	6862c656a13d14486e53e50cc875eef5c18f4dd0	9390714B1D909FA3D70DDC7681B38F07ED4E6356CB5C71915D1BDCD48FE335F8
CN = QuoVadis Swiss Regulated CA G2x 2.5.4.97 = NTRCH-CHE-112.210.349 O = QuoVadis Trustlink Schweiz AG C = CH	51fd54ae8897ca2e71bdf28655a6d515afff15c3	941B8AEE4BCF1EFEB0475FB279FDDDCF37FC5B20F64E842CD9DA0770B157E84D
CN = HydrantID Client ICA G2 O = HydrantID (Avalanche Cloud Corporation) C = US	330e34fc4ec99bc46d28edf7eea2f2e1787b5800	5286AE1C558A81537CD9870F749D96EFABC2D2BA393DF818DFE95EA7CE6450A7
CN = QuoVadis Issuing CA G4 O = QuoVadis Limited C = BM	7976e17ef17eaf5e19ea9e1b846512848fa8ba08	21B4B360A40EDC3C68A6EDA45765BB0B11EF491DCD5B96083FBD6C9FE84AA5E6
CN = Novartis Issuing CA by QuoVadis 2.5.4.97 = NTRCH-CHE-106.052.527 O = Novartis Pharma AG C = CH	221e3a1b63f88e99db9722817568af1cc453546d	0051C98924F239BD49AB8C8F6802F8B9CF4AD41EB3272F1A34C0CD6D61DCB3D4
CN = QuoVadis Swiss Advanced CA G2 O = QuoVadis Trustlink Switzerland Ltd. C = CH	494778a47dac511ccd03146d81e9afb344a55ace	554403B1F4A22D05525C0DD937916D441DF088598DCD4EFEF1676B09D0CA7824

Appendix B

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
1	In January 2019, QuoVadis disclosed previously addressed issues in 2018 certificate issuance: A. IP addresses in SAN dnsName fields B. Too many characters in Subject fields C. PrintableString contains invalid character	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link
2	QuoVadis disclosed previously addressed issues in 2018 certificate issuance at external subCAs. A. VR IDENT: Erroneous ISO country code	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link This link also includes QuoVadis' disclosures on other certificate issues related to: • Siemens – subject to its own ETSI audit • Freistaat Bayern – disclosed above in row 1 of this table • BIT – technically constrained Subordinate CA that has ceased issuance and moved to Managed PKI • DarkMatter – subject to its own WebTrust audit
3	QuoVadis disclosed issues related 3 errors in dnsNames for 8 certificates. A. Characters in labels of DNSNames MUST be alphanumeric, - , _ or * B. DNSName MUST NOT start with a period C. DNSNames should not have an empty label.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link

4	QuoVadis disclosed a number of certificates with invalid dnsNames containing IP addresses.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link
5	QuoVadis disclosed a certificate with invalid dnsNames containing IP addresses.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link
6	QuoVadis mistakenly disclosed an issue with s/MIME certificates having insufficient serial number entropy.	N/A – QuoVadis shared this in the interest of transparency and knowledge sharing.	Bugzilla Link
7	QuoVadis disclosed EV certificates issued with Organizationidentifier field in anticipation of CA/B Forum ballot SC17 coming into effect.	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2.	Bugzilla Link
8	QuoVadis disclosed EV certificates issued with "N/A" marked in the serialNumber field within the Subject of the certificate.	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2.	Bugzilla Link
9	QuoVadis disclosed issues relating to OCSP handling of Certificate Transparency pre-certificates.	N/A – QuoVadis shared this in the interest of transparency and knowledge sharing.	Bugzilla Link
10	QuoVadis disclosed that multiple EV certificates had Jurisdiction of incorporation (JOI) inconsistencies.	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2.	Bugzilla Link
11	QuoVadis disclosed an issue relating to non-disclosure of 18 ICAs technically capable of issuing TLS certificates in their WebTrust for Baseline Requirements (WTBR).	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link

12	QuoVadis disclosed that they issued intermediate CAs that do not conform to Mozilla's policies as it relates to extendedKeyUsage extension.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link
13	QuoVadis disclosed that multiple EV certificates had Jurisdiction of incorporation (JOI) inconsistencies. This is related to bug #10 above.	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2.	Bugzilla Link
14	QuoVadis disclosed their failure to reply in a timely manner on an issue related to EV certificates with wrong Business Category in the Subject field.	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2.	Bugzilla Link
15	QuoVadis disclosed an issue related to EV certificates with wrong Business Category in the Subject field. This is related to bug #14 above.	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2.	Bugzilla Link
16	QuoVadis disclosed failure to revoke 18 ICAs technically capable of issuing TLS certificates in the 5 days stipulated by the Baseline Requirements. This is related to bug #11 above.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link
17	QuoVadis disclosed certificates issued by external subCA LLB with insufficient serial number entropy.	WebTrust principles and criteria for certification authorities v2.1.	Bugzilla Link
Disclosures related to external subCAs that are not within the scope of this audit			
1	QuoVadis disclosed certificates issued by external subCA DarkMatter with insufficient serial number entropy.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link

2	QuoVadis disclosed certificates issued by external subCA Siemens with insufficient serial number entropy.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link
3	Disclosure to add QuoVadis external SubCAs operated by DarkMatter to OneCRL mechanism.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.	Bugzilla Link