



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 the SSL Certification Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.5** that provides its Certification Authority (CA) services at Bermuda, the Netherlands, Switzerland, the United Kingdom, Belgium and Germany, throughout the period 1 January 2021 to 31 December 2021 for CAs as enumerated in [Appendix A](#), QuoVadis has:

- ▶ Disclosed its SSL certificate lifecycle management business practices in its:
 - ▶ [QuoVadis Root CA 1 / Root CA 3 Certificate Policy / Certification Practice Statement, version 4.37](#) dated 20 December 2021 for the QuoVadis Root CA, QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3; and
 - ▶ [QuoVadis Root CA 2 Certification Policy/ Certification Practice Statement, v2.16](#) dated 20 December 2021 for the QuoVadis Root CA 2, QuoVadis Root CA 2 G3,

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements, 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 collected, authenticated (for the registration activities performed by Certification Authority (CA), Registration Authority (RA), and Subcontractor), and verified.
- ▶ 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 v2.5](#).

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 the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination

involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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 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.

QuoVadis' 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.

This report does not include any representation as to the quality of QuoVadis' CA services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network



Security v2.5 criteria, or the suitability of any of QuoVadis' services for any customer's intended purpose.

Ernst & Young LLP

Ernst & Young LLP

31 March 2022

**Management's Assertion Regarding the Effectiveness of Its Controls
Over the SSL Certification Authority Services
Based on the WebTrust Principles and Criteria for Certification Authorities -
SSL Baseline with Network Security v2.5**

31 March 2022

We, as the management of QuoVadis Limited (QuoVadis), are responsible for operating the SSL Certification Authority (CA) services at Bermuda, the Netherlands, Switzerland, the United Kingdom, Belgium and Germany for the Root CA(s) and Subordinate CA(s) in scope for SSL Baseline Requirements and Network Security Requirements listed at [Appendix A](#).

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 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 Bermuda, the Netherlands, Switzerland, the United Kingdom, Belgium and Germany throughout the period from 1 January 2021 through 31 December 2021, QuoVadis has:

- Disclosed its SSL certificate lifecycle management business practices in its:
 - [QuoVadis Root CA 1 / Root CA 3 Certificate Policy / Certification Practice Statement, version 4.37](#) dated 20 December 2021 for the QuoVadis Root CA, QuoVadis Root CA 1 G3, QuoVadis Root CA 3, and QuoVadis Root CA 3 G3; and
 - [QuoVadis Root CA 2 Certification Policy/ Certification Practice Statement, v2.16](#) dated 20 December 2021 for the QuoVadis Root CA 2, QuoVadis Root CA 2 G3,

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the QuoVadis 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 was established and protected throughout their lifecycles; and
 - SSL subscriber information was properly authenticated (for the registration activities performed by QuoVadis,
- 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 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,

for the Root CA(s) and Subordinate CAs in scope for SSL Baseline Requirements and Network Security Requirements at [Appendix A](#), based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.5](#).

Very truly yours,



Anthony Nagel
Director
QuoVadis Limited

Appendix A to Assertion of Management

Distinguished name	Certificate Serial Number	SHA-256 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	78585f2ead2c1 94be33707353 41328b596d46 593	8A866FD1B276B57E578E921C65828A2BED58E9F2F288054134B7F1F4BFC9CC74
CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM	509	85A0DD7DD720ADB7FF05F83D542B209DC7FF4528F7D677B18389FEA5E5C49E86
CN = QuoVadis Root CA 2 G3 O = QuoVadis Limited C = BM	445734245b81 899b35f2ceb82 b3b5ba726f075 28	8FE4FB0AF93A4D0D67DB0BEBB23E37C71BF325DCBCDD240EA04DAF58B47E1840
CN = QuoVadis Root CA 3 O = QuoVadis Limited C = BM	05c6	18F1FC7F205DF8ADDDEB7FE007DD57E3AF375A9C4D8D73546BF4F1FED1E18D35

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = QuoVadis Root CA 3 G3 O = QuoVadis Limited C = BM	2ef59b0228a7d b7affd5a3a9ee bd03a0cf126a1 d	88EF81DE202EB018452E43F864725CEA5FBD1FC2D9D205730709C5D8B8690F46
CN = HydrantID EV SSL CA G2 O = HydrantID (Avalanche Cloud Corporation) C = US	3c1e96137ee4 2057973ce498 cb50daae4c1e 3c48	60388B773D33E9141648613F36B9149F015A114378BACF3E3694864FFDA426EC
CN = HydrantID SSL CA G3 O = HydrantID (Avalanche Cloud Corporation) C = US	723b6fe5c2527 54d2189b0915 5521a3187916 db8	AA57F482CBC516B4D10CA4097DD90D99F5AA727D207090D07DA9C36998ABB9AD
CN = QuoVadis Grid ICA G2 O = QuoVadis Limited C = BM	2bafc5f0a8d21 3409da42e761f 619ac91984bc d4	278ECF211E2518E9DD9913AFC583EEB3127C8184BCBEEDAAD7BD64E89E8C4310
CN = QuoVadis Qualified Web ICA G2 O = QuoVadis Trustlink B.V. C = NL	53bd8dc20d4a 46bd962f5d685 ada0f0659207ff d	7FEB9374EAB08D392717C647436DAE06176A24C010607FDA1CCE5E5F0106B472

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = QuoVadis Global SSL ICA G2 O = QuoVadis Limited C = BM	1a6ee893c374 9738e12acc7 7a8c0acb167e af14	F67C23EF7BF7412809DB6B1DD3D44A08D3754D99CABA6A13F7A05C7249089C89
CN = VR IDENT EV SSL CA 2020 O = Fiducia & GAD IT AG C = DE	754151cc11ec 89b64649b230 ad809020bb1e 66a5	D33A847F640377BE0AE1A429153A07E87C8827FA4840B5158BCDCB85E10A453A
CN = HydrantID EV SSL ICA G1 O = HydrantID (Avalanche Cloud Corporation) C = US	0662a0088004 98fe4d810b24b b822d0bd23b9 0dc	6B43B4C243AA2D99440C0F14BDEC5231EEC63E86AAF2376CA7002028458DC726
CN = QuoVadis RCA1G3 TLS CA O = QuoVadis Limited C = BM	72348f4fb5967 e8409e6b0cce d6fa299b1ccd4 91	18BB70EFDA3F91438115C9EB4F333EB4EC68354571E6949195A0A91C9E6FBCD8
CN = DigiCert QV EV TLS ICA G1 O = DigiCert, Inc. C = US	65e9bcd53e79 1df22dffeb5ecc 2bc7a5588d08 83	6A7B2AA3414039A663D5D8BBAB8256A3979A84C332BF5E1EE8F6D0E0ADA84668

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = QuoVadis RCA3G3 TLS CA O = QuoVadis Limited C = BM	18dae051a897715eb0899ddcfb33b1cf0810eec0	ECC0D17AC3263AC6A164DCDB08F82D07E93FCEA723F66B88B06EEBA9678DF2BB
CN = QuoVadis Enterprise Trust CA 2 G3 O = QuoVadis Limited C = BM	5eeeb44a70e18e63c9898f202cbac164914edc05	174E1DE77C8D93C68ECD2BD2EA6E191B584DB850277A834AAC898B7C80A91C70
CN = QuoVadis Europe SSL CA G2 O = QuoVadis Trustlink B.V. C = NL	71aaaa628484114c591fd74b9fe9ffde5b29fa7e	B1AAE1BCD555E8A3D1E3DDA8EC84E757C552655344CE3FEEBBAF98E895DBEDAC
CN = QuoVadis RCA3G1 TLS CA O = QuoVadis Limited C = BM	2b07c16415396d53cd05f7a542cca4867e05c68d	3A66E648212E6321F94D9EABCC92C052E679D992C99AD4596A4E7B85ADCEE5DE
CN = QuoVadis Qualified Web ICA G3 O = QuoVadis Trustlink B.V. C = NL	2ca8cdc5b8ed750780c72e3392c9941c0ffb8826	3F225BDBCD788CE924870CAF92F814B7C6FF4EDABABAD93F1D3A9177252CF1D1

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = QuoVadis RCA1G1 TLS CA O = QuoVadis Limited C = BM	331dda8face8d 4b873dc8216f7 6affd0f5246e84	6BB964647B5EE6159A2A029EE5C7DCD1D9CF3B088451E0A68E90E6074C3F5CA3
CN = QuoVadis Global SSL ICA G2 O = QuoVadis Limited C = BM	48982de2a92c b339e1c8f9333 58275d3e4f882 55	A4879EC0F36CF84B6F2ED87AE57EE3B94A0785C6862238CD45481084D152EB18
CN = QuoVadis EV SSL ICA G3 O = QuoVadis Limited C = BM	3c71e6efc9462 1baec6e69329 0da08c615774 21f	ABB3FF299AA1BAEFC1278818C424388AEF7B29651595C60194E78D943694680B
CN = DigiCert QV TLS ICA G1 O = DigiCert, Inc. C = US	71520e460e54 aef322e39fac1 6c0e97a51bd9 572	93E33AF7DA3030530D090C9C55762CADE7EAE943F834349D1057A90EB67F306B
CN = QuoVadis Enterprise Trust CA 3 G3 O = QuoVadis Limited C = BM	0c2163a44924f fb7fcd675acd caee7208cca9 5a	DA5462526A0C2E9852A86186B025390158759CDCA6AE21F09F713CA6ACCDD1F1

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = QuoVadis Enterprise Trust CA 1 G3 O = QuoVadis Limited C = BM	0ad86fa335b93 ef48c8e3bf77d 4c63143643ad b9	0531C86F785958939FDC539924D395D1EFA409364E6827D3AB9876311FFB27B0
CN = QuoVadis Europe EV SSL CA G1 O = QuoVadis Trustlink B.V. C = NL	3a020322b681 6c18b72acbb5 92bef74dd786a 8b8	CB6666B32BFF2EFEDCC4187DF149A6D34A5D10B7165B9CFF2A67C0E311AEEED7
CN = VR IDENT SSL CA 2020 O = Fiducia & GAD IT AG C = DE	035fe137cd055 1e4c1f1b00beb a5aee53f95273 4	347D18DCCC2EFC51A920E7A7FBB07BFBDA35613681F82DCA5C4C72BB0C83C035
CN = QuoVadis EV SSL ICA G3 O = QuoVadis Limited C = BM	524fc1f16e34d 1702b84a13fb0 42bbcc7c3c903 2	F18442BEDF70B4D15211356C72B659332BED03FFD3BBA7AFAAABE6DE9D723002
CN = QuoVadis Enterprise Trust CA 2 G4 O = QuoVadis Trustlink B.V. C = NL	41d2651bf57da eec594226cf55 639c4c3285c2 4c	1E356823FE40C0EAAC29F9ED5463B7B2DB1C088B63EBB05876A2E631C1087798

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = HydrantID SSL ICA G2 O = HydrantID (Avalanche Cloud Corporation) C = US	7517167783d0 437eb556c357 946e4563b8eb d3ac	9C6D08933201407FBF2B12540B67CC0E4C9666F132E1504762A717CBAE8F3FD6
CN = QuoVadis Grid ICA G2 O = QuoVadis Limited C = BM	10b62f345a61e b6184a7b106c 8057e9453e20 7d5	74CE8C1631EF9F38E7A4197DA3F5474DBC34F001F2967C25B5999562BCC8C9D4
CN = QuoVadis Enterprise Trust CA 2 G3 O = QuoVadis Limited C = BM	31a84f278bbe4 a696e4cb2f415 a2e4473bdcca 38	B6F6559BBCE0A2CC91E507B5D7319E32487EDAE28A063BC73B6405E6C44665B6
CN = QuoVadis Issuing CA G4 O = QuoVadis Limited C = BM	69b2d1ccf02e2 0dcc95c62894f 7f9e5f5fc057bf	DA3BC81005FDBB853D681A7E942661AEBA23789211525EAF52221F28514C09CB
CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM	2d2c802018b7 907c4d2d79df7 fb1bd872727cc 93	30242443F6895A94560E48E4DFF720536EAF5163CB42F5E877402ABDE2F8627C

Distinguished name	Certificate Serial Number	SHA-256 Fingerprint
CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM	7ed6e79cc9ad 81c4c8193ef95 d4428770e341 317	CAB9C12DBDE3AD5D2BC0201B54B18BE209CD5E146AAA085ABBDF241B096DFF47
CN = HydrantID EV SSL ICA G1 O = HydrantID (Avalanche Cloud Corporation) C = US	5bfd1bb152d1 06baa6d6d17e 73c561f0dd9c8 ca	80FDE428212AF0CA0AC531EEE6ED2DF3D3C2A4557DFCE857070FC947922E9B24
CN = HydrantID SSL ICA G2 O = QuoVadis Limited C = BM	04E6881CFF6 CD65D5D554D 1839209CCEF AD7C78D	01453F645CD91E233B7484827F23F8A573FD641029EA8A6BFE549EF4ED8B323D
CN = QuoVadis Global SSL ICA G3 O = QuoVadis Limited C = BM	653247814F5F A66BB854DAF 053F329265D7 26538	161EE5386329B28A27FF405736552A621D5A844A43811E3623E52EEFA0BA840A

Appendix B

	Disclosure	Description	Relevant WebTrust Criteria	Publicly Disclosed Link
1	QuoVadis: revocation services validity set to expected value plus one second	QuoVadis OCSP services were off by one second because of the inclusive requirement of the start time.	WebTrust Principles and Criteria for: Certification Authorities v2.2.1, SSL Baseline with Network Security v2.5, and Extended Validation SSL, v1.7.3.	1733000
2	QuoVadis/PKloverheid: incorrect OCSP response for precertificate.	QuoVadis CMS requests a precertificate to be created by EJBCA but the CA unexpectedly rolls back the transaction, effectively removing the certificate from the CA database.	WebTrust Principles and Criteria for: Certification Authorities v2.2.1, SSL Baseline with Network Security v2.5, and Extended Validation SSL, v1.7.3.	1724276
3	QuoVadis: hostnames not in preferred name syntax	Hostnames not in preferred name syntax.	WebTrust Principles and Criteria for: Certification Authorities v2.2.1, SSL Baseline with Network Security v2.5, and Extended Validation SSL, v1.7.3.	1738472