QUOVADIS CODE-SIGNING CERTIFICATE SUBSCRIBER AGREEMENT

IMPORTANT: READ CAREFULLY

THIS QUOVADIS CODE-SIGNING CERTIFICATE SUBSCRIBER AGREEMENT ("AGREEMENT") IS ENTERED INTO BETWEEN THE SUBSCRIBER OF SUCH CERTIFICATE ("YOU," "THE APPLICANT" OR "THE SUBSCRIBER") AND QUOVADIS LIMITED ("QUOVADIS").

IF YOU ARE A SERVICE PROVIDER TO THE CONTENT ORIGINATOR AND WILL BE HOLDING THE CORRESPONDING PRIVATE KEY USED TO SIGN SUCH CONTENT, "SUBSCRIBER" INCLUDES YOU. YOU REPRESENT, WARRANT AND COVENANT THAT YOU HAVE FULL AGENCY AND AUTHORITY TO BIND THE CONTENT ORIGINATOR TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT BY YOUR ACCEPTANCE HEREOF, THAT BOTH OF YOU SHALL BE JOINTLY AND SEVERALLY LIABLE FOR THE PERFORMANCE HEREOF, THAT YOU SHALL PROCURE THE CONTENT ORIGINATOR'S FULL COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, AND THAT YOU HAVE OR WILL OBTAIN THE CONTENT ORIGINATOR'S PERMISSION TO DIGITALLY SIGN SUCH CONTENT.

ALL SUBSCRIBERS MUST FIRST READ THIS AGREEMENT AND AGREE, ACCEPT AND BE BOUND BY ITS TERMS. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, YOU ARE NOT AUTHORIZED TO BE THE SUBSCRIBER OF A QUOVADIS CODE-SIGNING CERTIFICATE AND YOU MUST TERMINATE YOUR APPLICATION OR REQUEST REVOCATION OF SUCH CODE-SIGNING CERTIFICATE. THIS AGREEMENT INCORPORATES BY REFERENCE ANY CERTIFICATE POLICIES CONTAINED IN THE QUOVADIS CODE-SIGNING CERTIFICATE AND CONDITIONS OF THE APPLICABLE QUOVADIS CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT ("CP/CPS") LOCATED AT http://www.quovadisglobal.com/repository.

THE USE OF A DIGITAL CERTIFICATE SIGNIFIES ACCEPTANCE OF THAT DIGITAL CERTIFICATE. BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS SUBSCRIBER AGREEMENT AND THE CP/CPS.

CAPITALIZED TERMS NOT DEFINED IN THIS AGREEMENT HAVE THE MEANING SPECIFIED IN THE CP/CPS.

QuoVadis and the Subscriber, intending to be legally bound, agree as follows:

1. ISSUANCE; FEES:

Upon the Subscriber's submission of a completed Application and QuoVadis' acceptance of that Application, QuoVadis shall issue the number of Code-Signing certificates applied for by the Subscriber. The Subscriber shall pay the then-current published price for such Code-Signing Certificate(s).

2. USE, PURPOSE AND LIMITATIONS:

The primary purpose of QuoVadis Trusted Code Signing Certificates is to establish that executable code originates from a source identified by QuoVadis. QuoVadis Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject. The Subscriber shall use the QuoVadis Code-Signing Certificate in accordance with the terms and conditions of this Agreement and the CP/CPS.

3. ROLE AND OBLIGATIONS OF QUOVADIS:

QuoVadis shall act as the Certification Authority for the QuoVadis Code-Signing Certificate and perform its obligations as specified in this Agreement and the CP/CPS. QuoVadis is not responsible or liable for the cryptographic methods used in connection with the QuoVadis Code-Signing Certificate. QuoVadis represents and warrants that it has followed the requirements of the CP/CPS in issuing the Code-Signing Certificate and

in verifying the accuracy of the information contained in the Certificate. QuoVadis may modify this Subscriber Agreement when necessary to comply with any changes to industry standards.

4.   ROLE AND OBLIGATIONS OF THE SUBSCRIBER:

Before accepting and using a QuoVadis Code-Signing Certificate, the Subscriber must: (i) generate its own Key Pair; (ii) submit an Application; and (iii) accept and agree to the terms of this Agreement. The Subscriber is solely responsible for the generation of the Key Pair to which the QuoVadis Code-Signing Certificate relates and for the protection of the Private Key underlying the QuoVadis Code-Signing Certificate. All Subscribers require a distinguished name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). The Distinguished Names of a Code Signing Certificate must identify the legal entity that intends to have control over the use of the Private Key when signing code. The Subscriber represents, warrants and covenants, so long as the Code-Signing Certificate is valid, that:

a) The Subscriber has provided/will provide truthful, accurate and complete information in all communications that refer, relate or pertain to the Code-Signing Certificate, including but not limited to all representations concerning identity of the Subscriber, application's name, information URL, application description, and all content digitally signed by the key corresponding to the Code-Signing Certificate, and as otherwise requested by QuoVadis. The Subscriber consents to QuoVadis retaining such registration information in accordance with the QuoVadis data retention policy;

b) The Subscriber will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy;

c) The Subscriber will take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Code-Signing Certificate(s) (and any associated access information or device e.g., password or token). This includes, but is not limited to, the implementation of adequate network and other security controls to protect against the misuse of the Private Key. The Subscriber confirms that one of the following options will be used to generate and protect its Code-Signing Private Keys:

   a. Recommended: A Trusted Platform Module (TPM) that generates and secures a Key Pair and that can document the Subscriber's Private Key protection through a TPM key attestation; or a hardware cryptographic module certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL4+, or equivalent; or

   b. Another type of hardware or storage token such as a SD card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL4+) if the Subscriber warrants that it will keep the token physically separate from the device that hosts the code signing function until a signing session has begun.

d) The Subscriber shall not apply for a Code-Signing Certificate if the Public Key in the Certificate is or will be used with a non Code-Signing Certificate.

e) The Subscriber will not install or use the Code-Signing Certificate(s) until it has reviewed and verified the accuracy of the data in each Code-Signing Certificate;

f) The Subscriber not use the Code-Signing Certificate(s) to digitally sign hostile code, spyware or other malicious software (this also includes disabling antispyware and other protective measures or providing false or misleading descriptions of the signed code's functions or features), and to use the Code-Signing Certificate solely in compliance with all applicable laws, solely for authorized purposes, and solely in accordance with the Subscriber Agreement;

g) The Subscriber will promptly cease using a Code-Signing Certificate and its associated Private Key, and promptly request that QuoVadis revoke the Code-Signing Certificate, in the event that: (a) any information in the Code-Signing Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the Code-Signing Certificate; or(c) there is evidence that the Cose-Signing Certificate was used to sign malicious code or software.

h) The Subscriber will promptly cease all use of the Private Key corresponding to the Public Key listed in a Code-Signing Certificate upon expiration or revocation of the Certificate.

i) As a best practice Subscribers should timestamp the digital signature after signing their code. QuoVadis operates an RFC3161 Time Stamp Authority (TSA). For further details please contact info@quovadisglobal.com.

j) The Subscriber acknowledges and accepts that, if: (a) the Certificate or the Subscriber is identified as a source of Suspect Code; (b) the authority to request the Certificate cannot be verified; or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.), then QuoVadis is authorized to share information about the Subscriber, application, Certificate, or surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

The Subscriber shall indemnify and hold harmless QuoVadis from any and all damages and losses arising out of: (i) use of a QuoVadis Code-Signing Certificate in a manner not authorized by QuoVadis; (ii) tampering with a QuoVadis Code-Signing Certificate; or (iii) any misrepresentations made during the use of a QuoVadis Code-Signing Certificate. In addition, the Subscriber shall indemnify and hold harmless QuoVadis from and against any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a QuoVadis Code-Signing Certificate relating to: (i) the Subscriber's breach of its obligations under this Agreement or the CP/CPS; (ii) the Subscriber's business and the use of or reliance upon a QuoVadis Code-Signing Certificate in connection with its business, it being acknowledged by the Subscriber that by entering into and performing its obligations under this Agreement, QuoVadis does not assume and should not be exposed to the Subscriber's business and operational risks; (iii) the Subscriber's failure to protect its Private Key; or (iv) claims (including without limitation infringement claims) pertaining to content or other information or data supplied by the Subscriber.

5. REVOCATION:

Certificates issued by QuoVadis will be revoked on the occurrence of any of the following events:

a) The Subscriber requests revocation of its Certificate;

b) The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;

c) QuoVadis obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised, or that the Certificate has otherwise been misused;

d) QuoVadis receives notice or otherwise become aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;

e) The Subscriber fails or refuses to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity;

f) QuoVadis receives notice or otherwise become aware that the Subscriber has used the Code-Signing Certificate to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers/phishing, or other content that is harmful, malicious, hostile or downloaded onto a user's system without their consent;

g) QuoVadis receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;

h) A determination, in QuoVadis' sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the CP/CPS or that that any of the information appearing in the Certificate is not accurate;

i) QuoVadis ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;

j) QuoVadis' right to issue Certificates by law, regulation, or policy expires or is revoked or terminated;

k) QuoVadis' Private Key for that Certificate has been compromised;

l) Such additional revocation events as QuoVadis publishes in its CP/CPS or deems appropriate based on the circumstances of the event; or

m) QuoVadis receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of QuoVadis' jurisdiction of operation.

n) Code signing certificates that have been revoked due to key compromise or that have been issued to unauthorized persons are maintained in QuoVadis' public revocation database for at least 20 years.

6.   DISCLAIMER OF WARRANTIES.

EXCEPT AS EXPRESSLY PROVIDED IN THE CP/CPS, QUOVADIS MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, RELATING TO ANY QUOVADIS CODE-SIGNING CERTIFICATE OR ANY RELATED SERVICES PROVIDED BY QUOVADIS, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

QuoVadis is not responsible or liable for the cryptographic methods used in connection with the QuoVadis Code-Signing Certificate.

7.   LIMITATION OF LIABILITY AND DAMAGES:

DESPITE ANY CONTRARY PROVISION CONTAINED IN THIS AGREEMENT OR THE CP/CPS, THE MAXIMUM LIABILITY OF QUOVADIS FOR ANY DAMAGES ARISING UNDER THIS AGREEMENT WILL NOT EXCEED US$250,000.

IN NO EVENT WILL QUOVADIS BE LIABLE TO THE SUBSCRIBER OR ANY THIRD-PARTY RELYING UPON OR OTHERWISE MAKING USE OF A QUOVADIS CODE-SIGNING CERTIFICATE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF QUOVADIS HAS BEEN ADVISED OF THE LIKELIHOOD OF THOSE DAMAGES IN ADVANCE.

THE SUBSCRIBER'S USE OF A QUOVADIS CODE-SIGNING CERTIFICATE IN A TRANSACTION WHERE THE POTENTIAL LIABILITY EXPOSURE IS GREATER THAN THAT CERTIFICATE'S MAXIMUM LIABILITY LIMIT AS SPECIFIED IN THIS SECTION 7 IS AT THE SUBSCRIBER'S OWN RISK.

8.   THIRD-PARTY BENEFICIARIES:

The Subject named in the Code-Signing Certificate, Microsoft and all other application software and operating system vendors with whom QuoVadis has entered into a contract for inclusion of the QuoVadis Root Certificate as a trusted root certificate in their software and all relying parties who actually rely on such Code-Signing Certificate during the period when the Certificate is valid are intended third party beneficiaries of this Agreement.

9.   TERM & TERMINATION:

This Agreement is effective upon QuoVadis' acceptance of the Subscriber's Application, and will terminate, except for those provisions which by their nature survive termination, upon the earliest of: (i) the latest expiration date of the QuoVadis Code-Signing Certificates issued to You under this Agreement; (ii) a breach of the Subscriber's obligations under this Agreement; (iii) the Subscriber's written request; or (iv) revocation of all QuoVadis Code-Signing Certificates issued to You under this Agreement.

10.   USER ID, PASSWORDS:

If the Subscriber receives a user id and/or password for purposes of accessing QuoVadis' web site, the Subscriber shall treat that user id and/or password as confidential information and shall only provide it to its employees who need to know.

11.   ASSIGNMENT:

The Subscriber shall not assign its rights or delegate its obligations under this Agreement or assign or delegate the QuoVadis Code-Signing Certificate to any third party. Any attempted assignment or delegation will be void. QuoVadis may assign its rights and delegate its obligations under this Agreement upon notice to the Subscriber.

12.   SEVERABILITY:

If any provision of this Agreement is declared or found to be illegal, unenforceable or void, that provision will be ineffective, but only to the extent that it is illegal, unenforceable or void, and will be amended to the extent necessary to make it legal and enforceable while preserving its intent. In addition, if the remainder of this

Agreement will not be affected by that declaration or finding and is capable of substantial performance, then each provision not so affected will be enforced to the maximum extent permitted by law. IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES OR EXCLUSION OF DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

13. GOVERNING LAW:

The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

- Dispute between the Root CA and an Issuing CA is dealt with under Bermuda Law.
- Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.
- Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing CA.

14. ENTIRE AGREEMENT, AMENDMENT:

This Agreement is the entire agreement between the parties and supersedes any and all prior or contemporaneous agreements or understandings between the parties regarding its subject matter. If there is any conflict between the provisions of this Agreement and the CP/CPS, the provisions of this Agreement will prevail. This Agreement may be amended or modified only by a written instrument executed by both parties.

15. FORCE MAJEURE:

QuoVadis is excused from performance under this Agreement and has no liability to the Subscriber or any third-party for any period when QuoVadis is prevented from performing all or part of its obligations, due to an act of God, war, civil disturbance, court order, labor dispute, or other similar event beyond QuoVadis' reasonable control.

16. NOTICES:

All notices provided by the Subscriber are considered given when in writing and delivered in hand by independent courier, delivered by registered or certified mail-return receipt requested, or sent by facsimile with receipt confirmed by telephone or other verifiable means, to:

QuoVadis Limited, Suite 1640, 48 Par La Ville Road, Hamilton HM11, Bermuda;

Website: www.quovadisglobal.com; Electronic Mail: compliance@quovadisglobal.com

YOU REPRESENT AND WARRANT THAT: (A) THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON THE SUBSCRIBER'S BEHALF AND TO BIND THE SUBSCRIBER TO THE TERMS OF THIS AGREEMENT; (B) SUBSCRIBER IS THE ENTITY THAT IT CLAIMS TO BE IN THE QUOVADIS CODE-SIGNING CERTIFICATE APPLICATION; (C) THE SUBSCRIBER HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT; AND (D) THIS AGREEMENT AND THE PERFORMANCE OF THE SUBSCRIBER'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE SUBSCRIBER IS A PARTY.