Relying Party Agreement for User Authentication Certificates

WHETHER YOU ARE AN INDIVIDUAL OR ORGANIZATION, YOU (“RELYING PARTY”) MUST READ THIS RELYING PARTY AGREEMENT FOR USER AUTHENTICATION CERTIFICATES ("AGREEMENT") EACH TIME BEFORE VALIDATING A SYMANTEC-ISSUED USER AUTHENTICATION CERTIFICATE [*1] (“SYMANTEC CERTIFICATE”) , USING SYMANTEC’S ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) SERVICES, ACCESSING OR USING A SYMANTEC DATABASE OF CERTIFICATE REVOCATIONS OR RELYING ON ANY INFORMATION RELATED TO THE SYMANTEC CERTIFICATE (COLLECTIVELY, "SYMANTEC INFORMATION”). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR RELY ON ANY SYMANTEC INFORMATION. IN CONSIDERATION OF YOUR AGREEMENT TO THESE TERMS, YOU ARE ENTITLED TO USE SYMANTEC INFORMATION AS SET FORTH HEREIN. AS USED IN THIS AGREEMENT, “SYMANTEC” MEANS SYMANTEC CORPORATION OR ANY OF ITS SUBSIDIARIES.

This Agreement becomes effective each time you submit a query to search for a Symantec Certificate, or rely on any Symantec Information in the manner set forth in the preamble above. This Agreement shall be applicable for as long as you use and/or rely on such Symantec Information.
A Certificate is an electronic credential that uses public key cryptography. Each holder of a Certificate has a public/private key pair. The private key, which is held securely by the holder, is used for creating digital signatures. The public key, which may be widely distributed, is used to enable others to verify digital signatures created by the holder of the private key. In order to rely on a public key, it is necessary that it be certified by an entity called a Certification Authority or CA. The CA binds a Subscriber’s public key to his or her identity, certifies the public key and creates an electronic credential called the Certificate. For purposes of this Agreement, CA means Symantec.

1. Definitions.

"Certificate Applicant" means an individual or organization that requests a Certificate from a Certification Authority.

"Registration Authority" or "RA" means an entity approved by a CA to assist Certificate Applicants in applying for, approving, rejecting, or revoking Certificates.

"Repository" means the collection of documents located at the link, which is accessible from the CA’s website.

"Subscriber" means a person, organization, or entity who is the subject of and has been issued a Certificate, and is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate

2. Informed Decision. You acknowledge and agree that: (i) you have sufficient information to make an informed decision as to the extent to which you choose to rely on the information in a Certificate; (ii) your use or reliance of any Symantec Information is governed by this Agreement and you shall bear the legal consequences of your failure to comply with the obligations contained herein. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A CERTIFICATE.

3. Your Obligations. As a Relying Party, you must ensure that your reliance on any Symantec Information is reasonable by: (i) assessing whether the use of a Certificate for any given purpose is appropriate under the circumstances; (ii) utilizing the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations you wish to perform, as a condition of relying on a Certificate in connection with each such operation; and (iii) checking the status of a Certificate you wish to rely on, as well as the validity of all the Certificates in its chain.

4. Limitations on Use. YOU ARE HEREBY NOTIFIED OF THE POSSIBILITY OF THEFT OR OTHER FORM OF COMPROMISE OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A CERTIFICATE, WHICH MAY OR MAY NOT BE DETECTED, AND OF THE POSSIBILITY OF USE OF A STOLEN OR COMPROMISED KEY TO FORGE A DIGITAL SIGNATURE. Symantec Certificates are not designed, intended, or authorized for use as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Class 1 Certificates [*2] shall not be used as proof of identity or as support of non-repudiation of identity or authority. Symantec, its CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate.

5. Compromise of Security. You shall not monitor, interfere with, or reverse engineer the technical implementation of the Symantec systems or otherwise intentionally compromise the security of the Symantec systems.

6. Symantec Warranties. Symantec warrants to Relying Parties who reasonably rely on a Certificate that (i) there are no material misrepresentations of fact in the Certificate known to or originating from Symantec; (ii) Certificates appearing in the Repository have been issued to the individual, organization or device named in the Certificate as the Subscriber; and (iii) the Certificate was issued in substantial compliance with the applicable Certification Practice Statement ("CPS") published at https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf or its successor URL. CPS is a document, as revised from time to time, representing a statement of practices that a CA

7. Disclaimers of Warranties. EXCEPT FOR THE EXPRESS LIMITED WARRANTIES CONTAINED IN SECTION 6, SYMANTEC DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSES, SATISFACTION OF CUSTOMER REQUIREMENTS, NON-INFRINGEMENT, AND ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. TO THE EXTENT JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN REPRESENTATIONS, WARRANTIES OR GUARANTEES, SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

8. Indemnity. You agree to indemnify, defend and hold harmless Symantec, any non- Symantec CA or RA, and any of their respective directors, shareholders, officers, agents, employees, successors and assigns from any and all third party claims, suits, proceedings, judgments, damages, and costs (including reasonable attorney's fees and expenses) arising from: (i) your failure to perform the obligations of a Relying Party in accordance with this Agreement; (ii) your reliance on a Certificate that is not reasonable under the circumstances; or (iii) your failure to check the status of a Certificate to determine if the Certificate is expired or revoked. Symantec shall promptly notify you of any such claim, and you shall bear full responsibility for the defense of such claim (including any settlements); provided however, that: (a) you keep Symantec informed of, and consult with Symantec in connection with the progress of such litigation or settlement; (b) you shall not have any right, without Symantec's written consent, which consent shall not be unreasonably withheld, to settle any such claim if such settlement arises from or is part of any criminal action, suit or proceeding or contains a stipulation to or admission or acknowledgement of, any liability or wrongdoing (whether in contract, tort, or otherwise) on the part of Symantec, or requires any specific performance or non-pecuniary remedy by Symantec; and (c) Symantec shall have the right to participate in the defense of a claim with counsel of its choice at its own expense. The terms of this Section 8 will survive any termination of this Agreement.

9. Limitations of Liability. THIS SECTION 9 APPLIES TO LIABILITY UNDER CONTRACT (INCLUDING BREACH OF WARRANTY), TORT (INCLUDING NEGLIGENCE AND/OR STRICT LIABILITY), AND ANY OTHER LEGAL OR EQUITABLE FORM OF CLAIM. TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYMANTEC SHALL NOT BE LIABLE FOR (I) ANY LOSS OF PROFIT, BUSINESS, CONTRACTS, REVENUE OR ANTICIPATED SAVINGS, OR (II) ANY INDIRECT OR CONSEQUENTIAL LOSS. SYMANTEC'S TOTAL LIABILITY FOR ALL DAMAGES SUSTAINED BY ALL RELYING PARTIES CONCERNING A SPECIFIC CERTIFICATE SHALL BE LIMITED, IN THE AGGREGATE, TO TEN DOLLARS ($10). THE LIABILITY LIMITATIONS PROVIDED IN THIS SECTION 9 SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE.
NOTWITHSTANDING THE FOREGOING, SYMANTEC'S LIABILITY SHALL NOT BE LIMITED UNDER THIS SECTION 9 IN CASES OF PERSONAL INJURY OR DEATH ARISING FROM SYMANTEC'S NEGLIGENCE OR TO ANY OTHER LIABILITY WHICH CANNOT BE EXCLUDED BY APPLICABLE LAW (INCLUDING MANDATORY LAWS OF ANY APPLICABLE JURISDICTION). TO THE EXTEND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN LIABILITY LIMITATIONS, SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

10. Severability. If any provision of this Agreement should be found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validty, legality and enforceability of the remaining provisions contained shall not, in any way, be affected or impaired thereby.

11. Governing Law. This Agreement and any disputes relating to the services provided hereunder shall be governed and interpreted according to each of the following laws, respectively, without regard to its conflicts of law provisions: (a) the laws of the State of California, if you are located in North America or Latin America; or (b) the law of England, if you are located in Europe, Middle East or Africa; or (c) the laws of Singapore, if you are located in Asia Pacific including Japan. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

12. Dispute Resolution. To the extent permitted by law, before you file suit or initiate an administrative claim with respect to a dispute involving any aspect of this Agreement, you shall notify Symantec, and any other party to the

dispute for the purpose of seeking business resolution. Both you and Symantec shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law as specified under this Agreement.

13. Non-Assignment. Except as stated otherwise, your rights under this Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights herein, whether by attachment, levy, garnishment or otherwise, renders this Agreement voidable at Symantec's option.

14. Notices. You will make all notices, demands or requests to Symantec with respect to this Agreement in writing to the "Contact" address listed on the website from where you purchased your Certificate, with a copy to: General Counsel – Legal Department, Symantec, 350 Ellis Street, Mountain View, California, USA 94043. References to telephone numbers above shall mean 1-650-527-8000.

15. Entire Agreement. This Agreement constitute the entire understanding and agreement between Symantec and you with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication relating thereto.

[*1] This is not a replying party agreement for SSL certificates. For an SSL certificate relying agreement, go to: http://www.symantec.com/content/en/us/about/media/repository/relying-party-agreement.pdf.

[*2] Symantec may offer three distinct classes of Certificates, with each class providing specific functionality and security features corresponding to a specific level of trust: (i) Class 1 Certificates. Class 1 Certificates offer the lowest level of assurance and should not be used for authentication purposes or to support non-repudiation. These certificates do not provide proof of the identity of the Subscriber. Class 1 Certificates are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is not necessary. (ii) Class 2 Certificates. Class 2 Certificates offer a medium level of assurance in comparison with the other two classes. Class 2 Certificates can be used for digital signatures, encryption, and access control, including as proof of identity in medium-value transactions. (iii) Class 3 Certificates. Class 3 Certificates provide the highest level of assurances. Class 3 Certificates are issued to individuals and organizations for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. Class 3 individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber to confirm his or her identity using, at a minimum, a well-recognized form of government-issued identification and one other identification credential. Class 3 organizational Certificates may be issued to devices to provide authentication; message, software, and content integrity; and confidentiality through encryption. Class 3 organizational Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has requested the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. Class 3 organizational Certificates also provide assurances that the Subscriber is entitled to use the domain name listed in the Certificate Application.