

**SYMANTEC TRUST NETWORK
RELYING PARTY AGREEMENT FOR SSL CERTIFICATES**

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES, INCLUDING GEOTRUST AND THAWTE ("COMPANY") IS WILLING TO PROVIDE THE SERVICES TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SERVICES (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS RELYING PARTY AGREEMENT ("AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE USING THE SERVICES. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND COMPANY. BY CLICKING THE 'ACCEPT', "I AGREE" OR "YES" BUTTON, OR USING THE SERVICES, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SERVICES. UNLESS OTHERWISE DEFINED HEREIN, CAPITALIZED TERMS WILL HAVE THE MEANING GIVEN IN THE "DEFINITIONS" SECTION OF THIS AGREEMENT AND SUCH CAPITALIZED TERMS MAY BE USED IN THE SINGULAR OR IN THE PLURAL, AS THE CONTEXT REQUIRES.

1. Services. Under the terms of this Agreement, You may i) submit a query to validate a Company Certificate, ii) use Company's Online Certificate Status Protocol (OCSP), iii) access or use a Symantec or Symantec-affiliated database of Certificate revocations, or iv) rely on Symantec Certificate related information (collectively "Symantec Information"). This Agreement shall be applicable for as long as You use and/or rely on such Symantec Information.

2. Definitions.

"Certificate" or **"Digital Certificate"** means a message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.

"Certificate Applicant" means an individual or organization that requests the issuance of a Certificate by a CA.

"Certificate Application" means a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

"Certification Authority" or **"CA"** means an entity authorized to issue, manage, revoke, and renew Certificates in the STN. For purposes of this Agreement, CA shall mean Company.

"Certification Practice Statement" or **"CPS"** means a statement of the practices that a CA or RA employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates. The CPS is published on the Repository.

"Non-verified Subscriber Information" means information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than the information was submitted by the Certificate Applicant.

"Operational Period" means the period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.

"Registration Authority" or **"RA"** means an entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke

Certificates, or renew Certificates.

"Relying Party" means an individual or organization that acts in reliance on a Certificate and/or a digital signature.

"Repository" means the collection of documents located at the website from which the Certificate was issued; specifically www.symantec.com, www.thawte.com, www.geotrust.com, or www.rapidssl.com.

"Subscriber" means in the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organization Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.

"Symantec Trust Network" or "STN" means the Certificate-based public key infrastructure governed by the Symantec Trust Network certificate policies, which enables the worldwide deployment and use of Certificates by Company, its affiliates, their respective customers, Subscribers and Relying Parties.

3. 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.**

4. Certificates. Company offers three (3) classes of certificate services, with each class providing specific functionality and security features corresponding to a specific level of trust within the STN, as further defined in the CPS:

(i) **Class 1 Certificates.** Class 1 Certificates offer a basic level of assurance and should not be used for authentication purposes or to support non-repudiation. 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. Class 1 Certificates are issued to individuals, and authentication procedures are based on assurances that the Subscriber's distinguished name is unique within the domain of a particular CA and that a certain email address is associated with a public key. These certificates do not provide proof of the identity of the Subscriber.

(ii) **Class 2 Certificates.** Class 2 Certificates offer a higher level of assurance in comparison with Class 1 Certificates. Class 2 Certificates can be used for digital signatures, encryption, and access control, including proof of identity in medium-value transactions. Under limited circumstances, Class 2 Certificates may be issued to an organizational Subscriber (rather than an individual within the organization). Such Certificates may be used for organization authentication and application signing only under the terms of the Symantec CPS. Class 2 Certificate authentication includes verification of information submitted by the Certificate Applicant against identity proofing sources.

(iii) **Class 3 Certificates.** Class 3 Certificates provide the highest level of assurance within the STN. Class 3 Certificates are issued to individuals and organizations for digital signatures, encryption, and access control, including proof of identity in high-value transactions. Class 3 Certificates issued to individuals provide assurance 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 Certificates issued to organizations may be issued to devices to provide authentication;

message, software, and content integrity; and confidentiality through encryption. Class 3 Certificates issued to organizations provide assurance 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 assurance that the Subscriber is entitled to use the domain name listed in the Certificate Application.

5. Your Obligations. As a Relying Party, You are obligated to ensure the reasonableness of Your reliance on any Symantec Information 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 upon which You intend to rely, as well as the validity of all the Certificates in its chain.

6. 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. Further, 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 shall not be used as proof of identity or as support of non-repudiation of identity or authority. Company, its CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate.

7. Compromise of STN Security. You shall not monitor, interfere with, or reverse engineer the technical implementation of the STN or otherwise intentionally compromise the security of the STN (unless You cannot be prohibited from so doing under applicable law), except upon prior written approval from Company.

8. Company Warranties. Symantec warrants to Relying Parties who reasonably rely on a Certificate that: (i) all information in the Certificate, except for Non-verified Subscriber Information, is accurate as of the date of Certificate issuance; (ii) Certificates 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 Symantec CPS.

9. Disclaimers of Warranties. EXCEPT FOR THE EXPRESS LIMITED WARRANTIES CONTAINED IN SECTION 8, COMPANY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTION OF YOUR REQUIREMENTS, NON-INFRINGEMENT, AND ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. COMPANY DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE. 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.

10. Indemnity. You agree to indemnify, defend and hold harmless Company, 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. Company 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: (i) You keep Company informed of, and consult with Company in connection with the progress of such litigation or settlement; (ii) You shall not have any right, without Company'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 Company, or requires any specific performance or non-pecuniary remedy by Company; and (iii) Company 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 10 will survive any termination of this Agreement.

11. Limitations of Liability.

11.1 THIS SECTION 11 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.

11.2 IF YOU INITIATE ANY CLAIM, ACTION, SUIT, ARBITRATION, OR OTHER PROCEEDING RELATING TO THIS AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, COMPANY SHALL NOT BE LIABLE FOR: (I) ANY LOSS OF PROFIT, BUSINESS, CONTRACTS, REVENUE OR ANTICIPATED SAVINGS, OR (II) ANY INDIRECT OR CONSEQUENTIAL LOSS.

11.3 COMPANY'S TOTAL LIABILITY FOR ALL DAMAGES SUSTAINED BY ALL RELYING PARTIES CONCERNING A SPECIFIC CERTIFICATE (OTHER THAN AN EXTENDED VALIDATION CERTIFICATE) SHALL BE DETERMINED ACCORDING TO THE CLASS OF THE CERTIFICATE RELIED UPON AND LIMITED, IN THE AGGREGATE, TO THE AMOUNT SET FORTH BELOW.

Class	Liability Cap
Class 1	One Hundred U.S. Dollars (US \$100.00) (or the local currency equivalent thereof)
Class 2	Five Thousand U.S. Dollars (US \$5,000.00) (or the local currency equivalent thereof)
Class 3	One Hundred Thousand U.S. Dollars (US \$100,000.00) (or the local currency equivalent thereof)

THE LIABILITY LIMITATIONS PROVIDED IN THIS SUBSECTION 11.3 SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE.

11.4 THIS SUBSECTION 11.4 APPLIES TO COMPANY SSL CERTIFICATES WITH EXTENDED VALIDATION ONLY: IF COMPANY FAILED TO ISSUE THE EXTENDED VALIDATION CERTIFICATE IN COMPLETE COMPLIANCE WITH THE EXTENDED VALIDATION GUIDELINES, THEN COMPANY'S LIABILITY FOR LEGALLY RECOGNIZED AND PROVEN CLAIMS SHALL BE LIMITED TO USD\$2000 PER RELYING PARTY PER CERTIFICATE.

11.5 NOTWITHSTANDING THE FOREGOING, COMPANY'S LIABILITY SHALL NOT BE LIMITED UNDER THIS SECTION 11 IN CASES OF PERSONAL INJURY OR DEATH ARISING FROM COMPANY'S NEGLIGENCE OR TO ANY OTHER LIABILITY WHICH CANNOT BE EXCLUDED BY APPLICABLE LAW (INCLUDING MANDATORY LAWS OF ANY APPLICABLE JURISDICTION). TO THE EXTENT JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF

CERTAIN LIABILITY LIMITATIONS, SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

12. General Provisions (Company Relying Party Agreement).

(a) **Notices.** You must make all notices, demands or requests to Company with respect to this Agreement in writing (excluding email) to the "Contact" address listed on the Repository, with a copy to the General Counsel – Legal Department, Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043, USA.

(b) **Entire Agreement.** This Agreement constitutes the entire understanding and agreement between Company and You with respect to the transactions contemplated hereunder, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication relating thereto.

(c) **Amendments and Waiver.** The observance of any term of this Agreement may be waived, only by writing in the form of a non-electronic record referencing this Agreement and signed by the parties to be bound thereby. Company may revise the terms of this Agreement at any time. Any such change will be binding and effective upon publication.

(d) **Force Majeure.** Neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder (excluding payment obligations) due to earthquake, flood, fire, storm, natural disaster, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott or other similar events beyond the reasonable control of such party, provided that the party relying upon this provision: (i) gives prompt written notice thereof, and (ii) takes all steps reasonably necessary to mitigate the effects of the force majeure event; provided further, that in the event a force majeure event extends for a period in excess of thirty (30) days in the aggregate, either party may immediately terminate this Agreement upon written notice.

(e) **Severability.** In the event that any provision of this Agreement should be found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions contained shall not, in any way, be affected or impaired thereby.

(f) **Compliance with Law.** Each party shall comply with all applicable federal, state and local laws and regulations in connection with its performance under this Agreement. You hereby acknowledge and agree that the technology You are accessing ("Controlled Technology") may be subject to applicable export control, trade sanction, and physical or electronic import laws, regulations, rules and licenses, and that You are hereby notified of the information published by Company on <http://www.symantec.com/about/profile/policies/legal.jsp>, or successor website, and will comply with the foregoing, and with such further export restrictions that may govern Controlled Technology, as specified in the relevant documentation. Company shall have the right to suspend performance of any of its obligations under this Agreement, without any prior notice being required and without any liability to You, if You fail to comply with this provision.

(g) **Assignment.** You may not assign the rights granted hereunder or this Agreement, in whole or in part and whether by operation of contract, law or otherwise, without Company's prior express written consent. Such consent shall not be unreasonably withheld or delayed.

(h) **Independent Contractors.** The parties to this Agreement are independent contractors. Neither party is an agent, representative, joint venturer, or partner of the other party. Neither party shall have any right, power or authority to enter into any Agreement for or on behalf of, or incur any obligation or liability of, or to otherwise bind, the other party. Each party shall bear its own costs and expenses in performing this Agreement.

(i) **Governing Law.** This Agreement and any disputes relating to the performance 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 a Customer is located in Asia Pacific including Japan. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

(j) **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 must notify Company, and any other party to the dispute for the purpose of seeking business resolution. Both You and Company must 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.

(k) **English Version.** If this Agreement is translated in any language other than the English language, and in the event of a conflict between the English language version and the translated version, the English language version shall prevail in all respects.

Symantec Trust Network Relying Party Agreement for SSL Certificates (April 2014)