

## Symantec™ Managed PKI Lite Public Service Agreement

This Symantec™ Managed PKI Lite Service Agreement ("Agreement") is entered into between Symantec (as defined below), and the entity listed at the bottom of this Agreement (referred to herein as "RA").

AS USED IN THIS AGREEMENT, "SYMANTEC" MEANS SYMANTEC CORPORATION AND ITS AFFILIATES.

This Agreement sets forth the terms and conditions applicable to RA who has purchased the Managed PKI Lite Service (formerly known as OnSite Lite) ("Service"). RA wishes to become an RA within the Symantec™ Subdomain of the Symantec™ Trust Network ("STN"). RA shall outsource to Symantec the functions of issuing, managing, revoking, and/or renewing Certificates, while retaining for itself the RA functions namely validating and approving Certificate Applications and requesting revocation or renewal of Client Certificates in accordance with the Symantec™ CPS and Managed PKI Administrator's Handbook.

**1. Definitions.** For the purposes of this Agreement, the following Capitalized terms will have the following meanings.

**"Administrator"** means a Trusted Person within an organization that performs validation and other CA or RA functions.

**"Administrator Certificate"** means a Certificate issued to an Administrator that may only be used to perform CA or RA functions.

**"Affiliated Individual"** means a natural person that is related to a given entity: (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of the Symantec™ registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.

**"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" ("CA")** means an entity authorized to issue, manage, revoke, and renew Certificates in the STN.

**"Erroneous Issuance"** means: (a) issuance of a Certificate in a manner not materially in accordance with the procedures required by the, the Managed PKI Administrator's Handbook or the RA Requirements; (b) issuance of a Certificate (other than a Class 1 Certificate) to a Subscriber other than the one named as the Subject of the Certificate; or (c) issuance of a Certificate (other than a Class 1 Certificate) without the authorization of the Subscriber named as the Subject of such Certificate.

**"Impersonation"** means requesting and being issued a Certificate based on false or

falsified information relating to naming or identity.

**"Intellectual Property Rights"** means all rights under one or more of the following: copyright, patent, trade secret, trademark, and any other intellectual property rights as defined in Section 7.1.

**"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.

**"Public Key Infrastructure" ("PKI")** means the architecture, organization, techniques, practices and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The STN PKI consists of systems that collaborate to provide and implement the STN.

**"RA Requirements"** means the summary of the security requirements applicable to Registration Authorities, which is located in the Managed PKI Administrator's Handbook.

**"RAA"** shall mean a Registration Authority Administrator who is an employee or Trusted Person of an RA that is responsible for carrying out the functions of an RA.

**"RAA Certificate"** shall mean a Registration Authority Administrator Certificate used to access the Managed PKI Control Center for the purpose of performing RA functions.

**"Registration Authority" ("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.

**"Subject"** means the holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.

**"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 organizational 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.

**"Subscriber Agreement"** is the agreement executed between a Subscriber and the CA relating to the provision of designated Certificate related Services and governing the Subscriber's rights and obligations relating to the Certificate.

**"Term"** shall have the meaning ascribed to it at Section 11 of this Agreement.

**"Trusted Person"** means an employee, contractor or consultant of an entity within the STN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities and/or its practices.

**"Symantec™ Affiliates"** means third parties, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with Symantec to be a STN distribution and services channel within a specific territory.

**"Symantec™ Trust Network" ("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 Symantec and the Symantec™ Affiliates, and their respective customers, Subscribers, and Relying Parties.

**2. Managed PKI Administrator's Handbook and RA Requirements.** The RA agrees to comply with the requirements of an RA as set forth in the Managed PKI Administrator's Handbook, as periodically amended. Symantec shall send e-mail notice to RA of any amendments, but shall have no obligation to confirm receipt of any such notice.

### **3. Symantec's Obligations.**

**3.1 Appointment.** Symantec appoints RA as a Registration Authority for the express purpose of issuing, managing and revoking Certificates per this Agreement.

**3.2 RAA Certificates.** Upon approval of the Certificate Application(s) of the RAA(s), Symantec shall issue an RAA Certificate to each such RAA. Such RAA Certificate(s) shall be valid for a period of twelve (12) months from the date of issuance.

**3.3 Certificate Issuance.** Upon RA's approval of a Certificate Application, Symantec: (i) shall be entitled to rely upon the correctness of the information in each such approved Certificate Application, (ii) shall issue a Certificate to the Certificate Applicant submitting such Certificate Application in accordance with RA's instructions and Symantec™ Certification Practice Statement ("CPS") then currently in effect, published on Symantec's website.

### **4. RA's Duties as a Registration Authority.**

**4.1 Appointments.** RA shall appoint one or more authorized RA employees or such other Trusted Persons as Registration Authority Administrator(s) ("RAA"). Specifically, RA hereby appoints the person(s) listed below as RAA(s). Such RAA(s) shall be entitled to appoint additional RAAs on RA's behalf.

**4.2 Registration Authority Requirements.** RA agrees to comply with the Registration Authority requirements stated in the Managed PKI Administrator's Handbook as periodically amended, including without limitation requirements for validating the information in Certificate Applications, approving or rejecting such Certificate Applications, using hardware and software designated by Symantec, and revoking Certificates. RA shall approve a Certificate Application only if the Certificate Applicant is an Affiliated Individual. If a Subscriber that has been issued a Certificate by RA ceases to be affiliated with RA as an Affiliated Individual, RA shall promptly request revocation of such Subscriber's Certificate. If an RAA ceases to have the authority to act as RAA on behalf of RA, RA shall promptly request revocation of the RAA Certificate of such RAA.

**4.3 Manner of Performance.** RA shall perform the tasks in this Section 4 in a competent, professional, and workmanlike manner.

**4.4 RA Employee Subscribers.** RA shall cause Subscribers receiving Certificates hereunder to abide by the terms of the Subscriber Agreement a copy of which can be located in the Managed PKI Administrator's Handbook. This Subscriber Agreement is also available in the enrollment process in the form of a "click-through" agreement and must be accepted before the enrollment is complete.

**4.5 Additional RA Obligations.** No information provided by RA (including RA's email

address) infringes the intellectual property rights of any third party; the Certificate Application information provided by RA (including RAA's e-mail address) has not been and will not be used for any unlawful purpose; RA has been (since the time of its creation) and will remain the only entity possessing RA's private key and no unauthorized person or entity has had or will have access to RA's private key; RA has been (since the time of its creation) and will remain the only entity possessing any challenge phrase, PIN, software, or hardware mechanism protecting RA's private key and no other person or entity has had or will have access to RA's private key; RA is using its Certificate as a Registration Authority and not as a Certification Authority; each digital signature created using RA's private key is RA's digital signature, and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created; RA will not monitor, interfere with, or reverse engineer the technical implementation of the STN, except with the prior written approval from Symantec; and Customer shall not otherwise compromise the security of the STN. RA shall bear exclusive responsibility and liability to any and all persons for the validation of all certificate applications that it approves and for the conduct of RAAs.

**4.6 Insurance Coverage.** RA shall, at its own expense, maintain standard errors and omissions insurance in an amount that is commercially reasonable. Upon Symantec's request, RA shall furnish proof of such insurance to Symantec.

**5. Fees and Payment Terms.** RA shall pay Symantec the then current applicable fees determined by Symantec corresponding to RA's selected volume of Certificates. RA shall pay any and all applicable value added or sales taxes or similar charges (except for taxes based on Symantec's income) relating to the products and services provided under this Agreement or to payments made by RA hereunder. All applicable fees are due immediately upon receipt by RA of an invoice from Symantec and are non-refundable. Payment of all applicable fees is a pre-requisite to the renewal of the Term of this Agreement. All payments under this Agreement will be made in U.S. dollars. All sums due and payable under this Agreement that remain unpaid after thirty (30) days from the date on which RA receives the corresponding invoice from Symantec will accrue interest as a late charge of 1.5% per month or the maximum amount allowed by law, whichever is less.

## **6. Confidentiality and Use of Information.**

**6.1 Confidential Information.** "Confidential Information" means any confidential or other proprietary information, including without limitation business, financial and technical information, disclosed by one party to the other under this Agreement, provided such information is identified as confidential at the time of disclosure and, if disclosed in tangible form, is marked "confidential" or "proprietary" or, if disclosed orally, is confirmed as being confidential in writing within a reasonable period of time (not to exceed thirty (30) days) after its initial disclosure, except that the following information is not Confidential Information: (a) information that is public knowledge at the time of disclosure, (b) information that becomes public knowledge or otherwise known to the receiving party after such disclosure, other than by breach of a confidentiality obligation, (c) information that was known by the receiving party before disclosure by the disclosing party, or (d) information that is independently developed by the receiving party without use of the disclosing party's Confidential Information.

**6.2 Protection of Confidential Information.** Each party will treat the Confidential Information of the other party as confidential, and with no less care than the party uses to prevent the disclosure of its own Confidential Information of like importance, but in no event less than reasonably diligent care. To the extent permitted by applicable law, the receiving party shall: (a) not disclose the Confidential Information to any third party, (b)

not use the Confidential Information in any fashion except for purposes of performing this Agreement, (c) exercise reasonable care to prevent disclosure, and (d) notify the disclosing party of any unauthorized disclosure or use of the Confidential Information of which the receiving party is aware. Upon termination of this Agreement for any reason, each party shall immediately deliver to the other party all copies of the Confidential Information received from the other party. Each party acknowledges that breach of this Section 6 may cause irreparable harm to the disclosing party entitling the disclosing party to seek injunctive relief, among other remedies. If return or destruction of the Confidential Information is not feasible, each party agrees to extend the confidentiality protections to limit any further use or disclosure until such time as the Confidential Information may be returned or destroyed.

**6.3. Disclosure Required by Law.** Notwithstanding the foregoing, a party may disclose the Confidential Information of the other party to the extent required by the order or requirement of a court, administrative agency or other governmental body if the party to disclose the other party's Confidential Information does the following: (a) gives written notice of the intended disclosure to the other party at least ten (10) days in advance of the date of disclosure or if ten (10) days is not feasible then as much notice as is possible under the circumstances; (b) upon request of the other party and at the requesting party's expense, the party to disclose the Confidential Information redacts portions of the Confidential Information to be disclosed to the extent permitted by applicable law; and (c) at the request and expense of the party whose Confidential Information is to be disclosed, submits a request to the court, administrative agency or governmental body that any portions of the Confidential Information that are identified by the other party receive confidential treatment to the fullest extent permitted under applicable law.

**6.4 Privacy.** Symantec will treat and process the data provided in any Certificate Application in accordance with the privacy statement specific to the Services ("Privacy Statement") as amended from time to time. RA agrees that Symantec may place in RA's Certificate certain information that RA provides for inclusion in its Certificate. In the case of individual Certificates, this information may include e-mail address and the name that RA gives Symantec to include in the Certificate. RA also agrees that Symantec may publish any Certificate issued under this Agreement and information about its status in Symantec's repository of Certificate information, make this information available to other repositories, and use such information for the purposes set out in this Agreement and in the Privacy Statement. RA warrants that RA has all necessary rights (including consents) to provide Subscriber information to Symantec. RA agrees that Symantec may process and/or transfer the information provided in any Certificate Application in the United States and in other jurisdictions where Symantec maintains a presence. For further information on processing of customer data, please see the applicable Privacy Statement, available at <http://www.symantec.com/about/profile/policies/privacy.jsp>.

## **7. Intellectual Property.**

**7.1 Intellectual Property Rights.** RA acknowledges that Symantec, its vendors, and/or its licensors retain all Intellectual Property Rights in and to the patents, copyrights, trade marks, service marks, trade secrets, ideas, concepts, techniques, inventions, processes, or works of authorship comprising or embodied in the products or services provided by Symantec hereunder, including without limitation the Symantec-designated hardware and software supporting such services and the web site interface designated for RA's use (collectively, the "Service Components"). The Service Components do not include RA's browser software or RA's base hardware platform. RA acknowledges that no title to the Service Components is transferred to it under this Agreement, and that it does

not obtain any rights, express or implied, in the Service Components, other than the rights that are expressly granted to RA in this Agreement. RA may not reverse engineer, disassemble or decompile the Service Components or make any other attempt to obtain the source code to the Service Components. To the extent RA creates any Derivative Work of any of the Service Components, such derivative work shall be owned by Symantec and all right, title and interest in and to such Derivative Work shall vest in Symantec. To the extent RA acquires any right to the Service Components or Derivate Works of the Service Components, RA hereby assigns to Symantec all right, title and interest in and to such Service Components and Derivative Works of Service Components. RA agrees to execute any assignment agreements or instruments as Symantec may request to vest in Symantec all such ownership rights.

**7.2 Proprietary Markings, Trademarks, Service Marks, Trade Names and Product Names.** RA shall not remove or destroy any trademark, copyright, patent or any other intellectual property notices on any Symantec materials, documentation or Service Components. Neither party shall acquire any rights of any kind in the other party's trademarks, service marks, trade names, or product names.

## **8. Warranties.**

**8.1 Symantec's Limited Warranties.** Symantec warrants to RA that: (a) there are no errors introduced by Symantec in RA's Certificate information and the Certificates issued by RA as a result of Symantec's failure to use reasonable care in creating the Certificate, (b) RA's Certificate complies in all material respects to the Symantec™ CPS, and (c) Symantec's revocation services and use of a repository conform to the CPS in all material aspects.

**8.2 RA's Warranties.** RA warrants to Symantec and anyone who relies on RA's Certificates that: (a) all information material to the issuance of a Certificate and validated by RA is true and correct; (b) RA's approval of Certificate Applications will not result in an Erroneous Issuance, including but not limited to an Erroneous Issuance resulting from Impersonation; and (c) RA has substantially complied with the CPS, the Managed PKI Administrator's Handbook and the RA Requirements.

**8.3 DISCLAIMER OF WARRANTIES.** SYMANTEC MAKES NO WARRANTIES, EXCEPT AS SET FORTH ABOVE AT SECTION 8.1 OF THIS AGREEMENT, AND THAT ALL OF SYMANTEC'S PRODUCTS AND SERVICES ARE PROVIDED ON AN "AS IS" BASIS, EXCEPT AS PROVIDED ABOVE AT SECTION 8.1 OF THIS AGREEMENT. EXCEPT FOR THE WARRANTIES SET FORTH AT SECTION 8.1 OF THIS AGREEMENT, SYMANTEC HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS AND IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SYMANTEC DOES NOT WARRANTY THAT THE SERVICES PROVIDED HEREUNDER WILL MEET RA'S REQUIREMENTS, BE UNINTERRUPTED, TIMELY OR ERROR FREE. TO THE EXTENT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY.

**9. LIMITATION OF LIABILITY.** THIS SECTION 9 APPLIES TO LIABILITY ARISING UNDER CONTRACT (INCLUDING WITHOUT LIMITATION BREACH OF WARRANTY), TORT AND ANY OTHER LEGAL OR EQUITABLE FORM OF CLAIM. IF RA INITIATES ANY CLAIM, ACTION, SUIT, ARBITRATION OR OTHER PROCEEDING RELATING TO SERVICES PROVIDED UNDER THIS AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYMANTEC'S TOTAL LIABILITY FOR DAMAGES SUSTAINED BY RA OR ANY THIRD PARTY FOR ANY USE OR RELIANCE ON A SPECIFIC CERTIFICATE SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNT PAID OR PAYABLE BY RA TO SYMANTEC FOR THE

SERVICE(S) PROVIDED HEREUNDER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO SUCH CLAIM. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL OR EXEMPLARY DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF DATA, GOODWILL, PROFITS, INVESTMENTS, USE OF MONEY OR USE OF FACILITIES, INTERRUPTION IN USE OR AVAILABILITY OF DATA, STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), ARISING OUT OF THIS AGREEMENT, THE SYMANTEC SERVICES, BREACH OF CONTRACT OR ANY EXPRESS OR IMPLIED WARRANTY, MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY, OR OTHER TORT. THE LIMITATION OF THIS SECTION 9 SHALL NOT APPLY TO EITHER PARTY'S GROSS NEGLIGENCE, WILLFUL, INTENTIONAL OR UNLAWFUL MISCONDUCT.

## **10. Indemnity.**

**10.1 Indemnity Obligations.** Subject to Section 9 of this Agreement, each party (the "Indemnifying Party") shall defend and indemnify the other party and its directors, officers, employees and contractors (collectively, the "Indemnified Parties") and hold the Indemnified Parties harmless from and against any losses, costs, damages, and fees (including reasonable attorneys' fees) incurred by the Indemnified Parties in connection with any claim or action brought by a third party to the extent based on: (a) any material breach by the Indemnifying Party of any warranty or obligation under this Agreement, the Managed PKI Administrator's Handbook, or the RA Requirements; (b) any material breach by the Indemnifying Party's acts or omissions; or (c) the use of any product or service provided by the Indemnifying Party, or any other item furnished by the Indemnifying Party to Subscribers.

**10.2 Indemnification Guidelines.** An Indemnified Party shall give the Indemnifying Party prompt written notice of any claim, suit, or proceeding for which the Indemnifying Party has an indemnification obligation under this Agreement. In the event such notice is not promptly given, the Indemnifying Party's obligation hereunder shall not include any additional expenses or damages to the extent attributable to such failure or delay of notice. An Indemnifying Party shall have the right to control and direct the investigation, preparation, defense, and settlement of the claim, and the Indemnified Party shall reasonably cooperate with the Indemnifying Party in the defense of such claim at the Indemnifying Party's expense. The Indemnifying Party may not settle any claim without the written consent of the Indemnified Party, which will not be unreasonably withheld or delayed. An Indemnified Party shall have the right to participate in the defense of any claim with its own counsel and shall be responsible for all costs associated therewith.

## **11. Term and Termination.**

**11.1 Term.** This Agreement will be in effect for one (1) year starting on the Effective Date (the "Initial Term"). This Agreement may be renewed for additional one (1) year terms (each a "Renewal Term") upon payment by RA to Symantec of the then applicable current fees determined by Symantec prior to the expiration of the Initial Term or then current Renewal Term, unless either party gives the other party at least thirty (30) days' notice of termination before the expiration of the then current Term. Notwithstanding the foregoing, Symantec expressly reserves the right to amend the terms of this Agreement for any Renewal Term by providing notice in the form of a written amendment or new Agreement at least thirty (30) days prior to expiration of the then current Term.

**11.2 Termination.** This Agreement may be terminated: (a) by either party immediately upon the institution by or against the other party of insolvency, receivership, or

bankruptcy proceedings; (b) by either party immediately upon any assignment for the benefit of the other party's creditors, or upon the other party's dissolution or ceasing to do business; (c) immediately by Symantec in the event RA compromises the security of Symantec's certification services or other systems RA or (d) in the event of a breach of this Agreement by a party, other than a breach by RA that compromises the security of Symantec's certification services or other system, upon thirty (30) days' advance written notice by the non-breaching party if the breaching party fails to cure such breach within the thirty (30) day notice period. This Agreement may be terminated by RA if Symantec amends the Managed PKI Administrator's Handbook, and if the RA believes in good faith that such amendment materially deprives it of the benefit of this Agreement.

**12. Notices.** Whenever a party desires or is required to give any notice, demand, or request with respect to this Agreement such communication shall be made in writing or using a digitally signed messages consistent with the requirements of this agreement (verifiable by a Class 2 or higher Certificate). Written notices must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, if to RA addressed to the representative of RA at the address below or if to Symantec at: Managed PKI Support, Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 with a copy addressed to Attention: General Counsel – Legal Department at the same address. RA shall immediately advise Symantec of any legal notice served on RA that might affect Symantec.

**13. Assignment.** RA 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 Symantec's prior express written consent. Such consent shall not be unreasonably withheld or delayed.

**14. Severability.** The unenforceability of any provision(s) of this Agreement shall not impair the enforceability of any other part of this Agreement. If any provision of this Agreement shall be deemed invalid or unenforceable, in whole or in part, this Agreement shall be deemed amended to delete or modify, as necessary, the invalid or unenforceable provision to render it valid, enforceable, and, insofar as possible, consistent with the original intent of the parties.

**15. 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 RA is located in North America or Latin America; or (b) the law of England, if RA is located in Europe, Middle East or Africa; or (c) the laws of Singapore, if RA 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.

**16. Dispute Resolution.** To the extent permitted by law, before RA files suit or initiate an administrative claim with respect to a dispute involving any aspect of this Agreement, RA shall notify Symantec, and any other party to the dispute for the purpose of seeking business resolution. Both RA 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.

**17. Force Majeure.** Except for payment and indemnity obligations hereunder, neither party shall be deemed in breach of this Agreement for any interruption or delay in the performance of its obligations under this Agreement due to forces beyond its control, including without limitation earthquakes, fires, floods, natural disasters, armed conflicts or terrorist actions (a "Force Majeure Event"), provided that the party whose



performance is interrupted or delayed (the "Affected Party") give the other party (the "Unaffected Party") prompt written notice of the Force Majeure Event. In the event the Affected Party's performance of its obligations is delayed by more than thirty (30) days or is interrupted for a period greater than thirty (30) days as a result of the Force Majeure Event the Unaffected Party may immediately terminate this Agreement by providing a written notice of termination to the Affected Party.

**18. Export Law Compliance.** This Agreement is expressly made subject to any laws, regulations, orders or other restrictions on the export from the United States of America of software, hardware, or technical information, which may be imposed from time to time by the government of the United States of America. Regardless of any disclosure made by RA to Symantec of an ultimate destination of the software, hardware, or technical information and, notwithstanding anything contained in this Agreement to the contrary, RA shall not export, or re-export, either directly or indirectly, any software, hardware, or technical information, or portions thereof, without first obtaining any and all necessary licenses from the United States government or agencies or any other country for which such government or any agency thereof requires an export license or other governmental approval at the time of modification, export, or re-export. RA shall be deemed to be the importer of record of any software provided to RA outside of the U.S., and shall be responsible for any related import filings, requirements, documentation, fees, taxes, duties, or other compliance obligations imposed by the applicable destination country or jurisdiction. RA also agree that RA will not use the software, hardware, or technical information for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of nuclear, missiles, or chemical or biological weapons.

**19. Independent Contractors.** The parties to this Agreement are independent contractors. Neither party is an agent, representative, 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. This Agreement shall not be interpreted or construed to create an association, joint venture or partnership between the parties or to impose any partnership obligation or liability upon either party. Each party shall bear its own costs and expenses in performing this Agreement.

**20. Headings.** The section and paragraph headings appearing in this Agreement are inserted only as a matter of convenience and in no way define, govern, limit, modify or construe the scope or extent of the provisions of this Agreement to which they may relate. Such headings are not part of this Agreement and shall not be given any legal effect.

**21. Modifications.** No modifications to this Agreement shall be accepted unless Symantec has first agreed to the modification and counter-signed the Agreement.

**22. Survival.** The provisions of Sections 1, 2, 5 (with respect to fees incurred as of the effective date of termination), 6, 7, 8, 9, 10, 11, 12, 13, and 14 shall survive the termination or expiration of this Agreement.

**23. Approval; Authorization.** This Agreement shall not be effective until the RA executes this Agreement and Symantec approves RA's Registration Authority application. RA and Symantec represent and warrant that the representative executing this Agreement on their behalf have been duly authorized by them to do so.

**24. Entire Agreement; Amendment; Waiver.** This Agreement, the Managed PKI Administrator's Handbook and the RA Requirements constitute the entire agreement

between the parties and supersede all prior and contemporaneous written or oral agreements between the parties with respect to the subject matter of this Agreement. No amendment of any provision of this Agreement shall be effective unless it is in a writing signed by each party's authorized representative. This Agreement may not be amended by any purchase order. Except with respect to price, quantity and billing address information terms that are mutually agreed upon by the parties, all terms and conditions in any purchase order are null and void. Symantec's accepting and processing a purchase order containing terms and conditions that are not contained in this Agreement or that are inconsistent with this Agreement will not be deemed as Symantec's acceptance of those terms or conditions. All purchase orders issued in connection with this Agreement will be governed exclusively by the terms and conditions of this Agreement. No waiver of any right under this Agreement shall be effective unless it is in a writing signed by the waiving party. The failure of a party, at any time or from time to time, to require performance of any obligations of the other party hereunder shall not affect its right to enforce any provision of this Agreement at a subsequent time.

**ACCEPTED AND AGREED TO:**

**RA:** \_\_\_\_\_  
(Name of company or entity)

Address: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

By: \_\_\_\_\_  
(Signature)

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
E-Mail: \_\_\_\_\_  
Voice: \_\_\_\_\_  
Fax: \_\_\_\_\_

**RAA's APPOINTED BY RA:**

**1. First RAA (required)**

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
E-Mail: \_\_\_\_\_  
Voice: \_\_\_\_\_  
Fax: \_\_\_\_\_

**2. Second RAA (optional)**

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
E-Mail: \_\_\_\_\_  
Voice: \_\_\_\_\_  
Fax: \_\_\_\_\_