Symantec™ Managed Public Key Infrastructure (PKI) Service Description

Introduction

Symantec™ Managed Public Key Infrastructure (PKI) service provides a flexible PKI platform to manage the complete certificate lifecycle to issue new certificates, renew existing certificates, and revoke untrustworthy certificates. Additionally, this service provides the ability to escrow and recover private keys of certificates used to encrypt emails, file systems, or other data. Further, this service offers numerous validation services to verify certificates’ current status to ensure only trustworthy certificates perform such actions as encrypting data, digitally signing documents, or authenticating onto networks.

As a managed service, Symantec Managed PKI significantly reduces costs associated with an in-house PKI. For example, customers need to acquire cryptographic and application server hardware, purchase server and client licenses, and train staff before issuing the first certificate from an in-house PKI deployment. Further, customers have to create their own certificate policy (CP) as a principal statement of policy governing the PKI hierarchy, and certification practices statement (CPS), which defines certificate process and procedures as well as trusted roles and responsibilities. Symantec Managed PKI service is designed as multi-tenant, highly-available environment based on best-of-breed cryptographic and application server hardware. Additionally, this environment is monitored 24x7x365 by a professionally trained staff that has passed enhanced security background checks. Further, this environment is audited on a regular basis to maintain WebTrust and SAS70 accreditation.

This service description outlines the primary features of Symantec Managed PKI service:

Certificate Authority (CA)

Symantec Managed PKI service creates and manages Certificate Authority (CA) hierarchies:

- **Standard CA Hierarchies**

  Symantec Managed PKI service includes the following CA hierarchies: Symantec Trust Network (STN), Private Certificate Authority, and Adobe® Certified Document Services (CDS). Please refer to Appendix A, Appendix B, and Appendix C for specific STN, Private Certificate Authority, and Adobe CDS terms and conditions, respectively.

Certificate Lifecycle Management

Symantec Managed PKI service offers two (2) deployment models, Cloud and Hybrid, to manage certificate lifecycle. The Cloud deployment model hosts account, certificate, and key management tools in Symantec’s data centers. The Hybrid deployment model also hosts all account, certificate, and key management tools in Symantec’s data centers, but this model installs registration authority (RA) and directory integration tools in the customer’s data center as well. The deployment models are not exclusive and can use a combination of deployment models based on the needs of various PKI projects. Further, both deployment models work with desktop middleware, PKI Client, designed to dramatically improve the user experience with the certificate lifecycle. Below is a description of these tools:

- **PKI Manager**

  PKI Manager is a web portal hosted in Symantec’s data centers for a PKI administrator to perform tasks related to account, user, certificate, and key management.

  o **Account Management**

    PKI Manager enables a PKI administrator to view certificate authorities (CAs), number of seats, and reports associated with their account(s). In addition, PKI Manager allows a PKI administrator to create and assign responsibilities to additional PKI administrators.
- **User Management**

  PKI Manager permits a PKI administrator to add users, generate unique passcodes for each user, and customize emails sent to users. Additionally, PKI Manager has the capability to provide users with document and video-based instructions to configure third party applications to work with the newly-issued certificates.

- **Certificate Management**

  PKI Manager enables a PKI administrator to configure certificate profiles for different CAs in their account. As part of these certificate profiles, a PKI administrator sets such parameters as key sizes, key usages, and signing algorithms. A PKI administrator also selects user experience (native or PKI Client) and security protection level. Further, a PKI administrator decides whether or not to escrow private keys of the certificates. Along with configuring certificate profiles, PKI Manager lets a PKI administrator revoke certificates which have become untrustworthy because a user no longer needs a certificate (i.e., a user left the company) or a private key has been comprised (i.e., a user lost a laptop.).

- **Key Management**

  PKI Manager provides a PKI administrator with the ability to recover a private key of an encryption certificate.

### PKI Certificate Service

PKI Certificate Service hosts the certificate enrollment web pages in Symantec’s data centers for users (a.k.a., subscribers) to request certificates. These web pages guide users through the necessary steps to request certificates. In addition, these web pages may display instructions, provided by a PKI administrator, to configure third-party products.

### Certificate Issuance Center

Certificate Issuance Center is the certificate engine hosted in Symantec’s data centers. This certificate engine creates certificates based on certificate signing requests submitted from PKI Certificate Service, received from PKI Enterprise Gateway, or sent via Web Services. Additionally, this certificate engine signs these certificates with the issuing Certificate Authority (CA).

### PKI Enterprise Gateway

PKI Enterprise Gateway is a registration authority (RA) authority application installed in the customer’s data center, if desired. This application tightly integrates with a Lightweight Directory Access Protocol (LDAP) source (i.e., Microsoft® Active Directory®) to automatically approve certificate requests and publish certificate data back into the LDAP source.

### PKI Client

PKI Client is an endpoint middleware designed to dramatically improve user experience with the certificate lifecycle. PKI Client is available for desktops on Windows as well as MAC operating systems. In the native experience, users use either Microsoft Internet Explorer® or Mozilla® Firefox® to request certificate from certificate enrollment web pages. While this native experience does not require any additional software, the native experience has known usability limitations. For example, Microsoft Internet Explorer produces numerous pop-up windows with warning messages that often confuse users. In the PKI Client experience, the certificate lifecycle has been streamlined to automate common functions (i.e., certificate renewal) to minimize user involvement. PKI Client also provides centralized policy management functions (e.g., PIN, export, etc.) to protect certificates. Further, PKI Client has the ability to auto-configure third-party products (e.g., wireless, virtual private network clients, etc.) to use certificates. Symantec Managed PKI Certificate lifecycle management functions are also available on mobile devices such as the iOS that leverages built-in iOS Over-the-Air (OTA) protocol capabilities. This allow the iOS device or application to make certificate enrollment requests via Apple’s SCEP protocol. For mobile operating systems such as the Android OS, that don’t have an iOS OTA equivalent, Symantec provides a PKI Client that similarly hides the complexity of configuring the device and application to use the certificate.

### PKI Web Services

Symantec Managed PKI Service Description (February 2013)
PKI Web Services hosted in the Symantec data center provide the capability to programmatically integrate with Symantec Managed PKI. A third party application can obtain a certificate policy and perform certificate lifecycle functions such as enroll and renew using the API provided by PKI Web Services.

**Authentication Methods**

*Symantec Managed PKI* service offers the following authentication methods:

- **Authentication using Enrollment Code**

  With this type of authentication, a PKI administrator can generate a unique enrollment code for each user in order to automatically approve certificate requests. When a PKI administrator sends certificate invitations to users with a link to certificate enrollment web page, the PKI administrator includes the unique passcode for that user. Users then include their passcode along with any additional information in the certificate enrollment web pages. Certificate Issuance Center compares this enrollment code to the information generated in PKI Manager. If there is a match, Certificate Issuance Center issues a certificate. If the user-entered enrollment code does not match the one that was generated for that user, Certificate Issuance Center gives an error message to the user.

- **Automated Authentication**

  Automated authentication approves certificate requests based on data in a LDAP source (i.e., *Microsoft Active Directory*). PKI Enterprise Gateway must be installed in a customer’s data center and integrated with an LDAP source. When users submit certificate requests via PKI Certificate Service, PKI Enterprise Gateway compares the data in the certificate requests with the LDAP source. If data match, PKI Enterprise Gateway approves certificate requests, signs certificate requests with Registration Authority (RA) certificate, and sends signed certificate requests to Certificate Issuance Center. Else, PKI Enterprise Gateway rejects certificates requests.

**Certificate Validation**

*Symantec Managed PKI* service provides the following certificate validation tools:

- **Certificate Revocation List (CRL)**

  Many third-party products have the ability to check the certificate’s current status (e.g., active, revoked, etc.) through Certificate Revocation List (CRL). A CRL is a black list of revoked certificates that have not yet expired. These products can be configured to download and check most recent CRL on a regular basis. If a certificate appears on the CRL, these products deny access (e.g., will not authenticate onto networks, digitally sign documents, etc.). Symantec produces a CRL at least once every 24 hours.

- **Online Certificate Status Protocol (OCSP)**

  Many third-party products verify the current status of certificates (e.g., active, revoked, etc.) via Online Certificate Status Protocol (OCSP). While all revoked certificates will appear on a CRL, there is a time delay between the certificate’s revocation and next CRL run which may be up to 24 hours for a standard CRL. Symantec immediately updates the certificates’ status upon any change (e.g., revoked, suspended, etc.) which is reflected in near-real time within Symantec’s OCSP tool, Trusted Global Validation (TGV).

**Hardware Options**

Symantec resells the following hardware options to complement *Symantec Managed PKI* service:

- **Aladdin PKI Tokens**

  Symantec is an authorized reseller of *Aladdin eToken* series which includes PRO, NG-OTP, and NG-FLASH tokens. In addition, these tokens also come with a three (3)-year warranty as described in the Warranty Information Supplement. Further, these tokens meet Federal Information Processing Standard (FIPS) 140-2 and Common Criteria standards.
• SafeNet Hardware Security Modules (HSMs)

Symantec is an authorized reseller of SafeNet® Luna® hardware security modules (HSMs) which consists of Luna® PCI cards, Luna® SA network appliances, and Luna® PCM tokens. While these HSMs include a one (1) year basic warranty, Symantec resells optional SafeNet extended warranty programs for additional charge. These HSMs also meet FIPS 140-2 Level 2 and Common Criteria standards.

Support and Maintenance

The support and maintenance commitments of Symantec are described in the applicable Service Level Agreement.

If you use the Microsoft Auto-enrollment component of the Symantec MPKI service, then the following MICROSOFT REQUIRED SUPPLEMENTAL OBLIGATIONS shall apply:

(a) Disclaimer of WARRANTIES. MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AS TO THE SERVER SOFTWARE PROVIDED HEREUNDER (“SERVER SOFTWARE”), AND HAVE NO RESPONSIBILITY FOR ITS PERFORMANCE OR FAILURE TO PERFORM. AS TO MICROSOFT, THE SERVER SOFTWARE IS PROVIDED AS IS AND WITH ALL FAULTS, AND MICROSOFT AND ITS AFFILIATES HEREBY DISCLAIM ALL OTHER WARRANTIES, DUTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, ALL WITH REGARD TO THE SERVER SOFTWARE. ALSO, MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SERVER SOFTWARE.

(b) Exclusion of Certain Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SERVER SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SERVER SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SERVER SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY OF THESE SERVICE DESCRIPTION TERMS AND CONDITIONS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF MICROSOFT, AND EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(d) Third Party Beneficiary. Notwithstanding any inconsistent terms of the Agreement, Customer hereby agrees that Microsoft Corporation, as a licensor of intellectual property included in the Server Software, is intended to be a third party beneficiary of these Service Description terms and conditions with rights to enforce any terms therein that affect any included Microsoft intellectual property or other Microsoft interest related to the terms hereof.

(e) Server Class 2. If Customer has elected the Server Class 2, Customer may use the Server Software on a server that (a) contains not more than four (4) processors, where each such processor has a maximum of thirty-two (32) bits and four (4) gigabytes of RAM, and (b) is not capable of having memory added, changed or removed without the requirement that the server on which it is running be rebooted (“Hot Swapping Capabilities”). Customer may not use the Server Software in conjunction with any software that supports Hot Swapping Capabilities or Clustering Capabilities, where “Clustering Capabilities” means the ability to allow a group of servers to function as a single high-availability platform for running applications using application failover between Server nodes in the group.

(f) Audit Rights. Symantec may audit Customer and inspect Customer’s facilities and procedures during regular business hours at Customer premises upon not less than fourteen (14) days’ notice to verify Customer’s compliance with all terms and conditions hereof. Notwithstanding any inconsistent terms of the Agreement (including without limitation any confidentiality provisions), should Customer refuse to undergo such audit and Symantec has reason to believe Customer may not be in compliance with the Service Description terms and conditions, Customer agrees that Symantec may disclose to Microsoft Customer’s identity and the basis for Symantec’s belief of non-compliance.

Symantec Managed PKI Service Description (February 2013)
(g) **Multiplexing Devices.** Hardware or software that reduces the number of users directly accessing or using services provided by the Server Software does not reduce the number of users deemed to be accessing or using services provided by the Server Software. The number of users accessing or using the Server Software is equal to the number of users who access or use, either directly or through a Multiplexing Device, services provided by (a) the Server Software or (b) any other software or system where the authentication or authorization for such software or system is provided by the Server Software (an “Other Authenticated System”). As used here, a “Multiplexing Device” means any hardware or software that provides or obtains access, directly or indirectly, to services provided by the Server Software or any Other Authenticated System to or on behalf of multiple other users through a reduced number of connections.

(h) **Windows CAL Requirement.** Customer must acquire and dedicate a separate Windows CAL for each user that is accessing or using, either directly or through or from a Multiplexing Device, services provided by the Server Software or any Other Authenticated System. A “Windows CAL” means (a) a Windows Device Client Access License (“CAL”), or a Windows User CAL, in either case for a Microsoft Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) server operating system product (or any successors thereto) (“Windows Server”); or (b) a Microsoft Core CAL that provides an individual person or electronic device with rights to access and use Windows Server, in either of (a) or (b) above that Customer has acquired for use with one or more such Microsoft Windows Server operating system products or electronic device and that is used on a per user or per device basis.

*Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Norton, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.*
Appendix A: Symantec Trust Network (STN)

Symantec™ Managed Public Key Infrastructure (PKI) service provides customers with the ability to issue certificates from the Symantec Trust Network (STN). Symantec has worked with hardware and software vendors to embed the STN Primary Certificate Authorities (PCAs) into the most popular web browsers, email applications, operating systems, and network appliances. As a result, certificates chaining to one of these PCAs are automatically trusted by these applications. These certificates can generally be used across organizations without any special preparation by either administrators or users. For example, many customers use STN certificates for secure email which digitally signs and/or encrypts email.

Every customer is automatically provisioned an issuing Certificate Authority (CA) chaining to Class 2 PCA as part of standard package. If a customer wants another trademarked name or change any of the default values in the CA, the customer may purchase an option to create additional CAs.

Note: Customers and user must adhere to the Symantec Trust Network Certification Practice Statement (CPS) to issue, manage, and use these certificates.

SERVICE TERMS AND CONDITIONS FOR SYMANTEC TRUST NETWORK

1. DEFINITIONS
“Administrator Certificate” means the Certificate issued by Symantec to the Customer employee or such other Trusted Person designated as the Managed PKI Administrator for the sole purpose of accessing the PKI Manager to perform Administrator functions.
“Affiliated Individual” means a person that is affiliated to Customer: (a) as an officer, director, employee, partner, contractor, intern, or other person within Customer’s organization; or (b) as a person maintaining a contractual relationship with Customer’s organization where Customer has business records providing strong assurances of the identity of such person.
“Agreement” means the Professional Services Agreement or such other master agreement entered into between Symantec and Customer under which the Services Order applicable to this Service Description is issued.
“Certificate” or “Digital Certificate” means a message that, at least, states a name or identifies the issuing CA, identifies the Subscriber, contains the Subscriber’s Public Key, identifies the Certificate’s Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing CA.
“Certificate Applicant” means a person or authorized agent that requests the issuance of a Certificate by a CA.
“Certificate Application(s)” means a request from a Certificate Applicant (or authorized agent) to a CA for the issuance of a Certificate.
“Certificate Signing Unit” or “CSU” means a hardware unit or software designed for use in signing Certificates and key storage.
“Certification Authority” or “CA” means a person or entity authorized to issue, suspend, or revoke Certificates.
“Certification Practices Statement” or “CPS” means a document, as revised from time to time, representing a statement of the practices a CA or RA employs in issuing Certificates. The STN CPS is published in the repository on the Symantec website.
“Erroneous Issuance” means (a) issuance of a Certificate in a manner not materially in accordance with the procedures required by the STN CPS, (b) issuance of a Certificate to a person other than the one named as the subject of the Certificate, or (c) issuance of a Certificate without the authorization of the person named as the subject of the Certificate.
“Key Generation” means the Symantec procedures for proper generation of Customer CA Public Key and Private Key via a trustworthy process and for storage of the Private Key and documentation thereof.
“Managed PKI Administrator” means an employee of the Registration Authority or such other Trusted Person authorized to perform RA tasks.
“Operational Period” means a 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 a date and time at which the Certificate expires or is earlier revoked.
“Private Key” means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.
“Public Key” means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.
“Registration Authority” or “RA” is an entity that performs identification and authentication of Certificate Applicants for Certificates, initiates or passes along revocation requests for Certificates, or approves applications for renewal or re-keying of Certificates. A RA is not an agent of a Certificate Applicant. A RA may not delegate the authority to approve Certificate Applications other than to authorized Managed PKI Administrators of the RA.
“Seat” means a single Subscriber that is an authorized end user of the service, without regard to the number of Certificates actually issued to that Subscriber.

“Subscriber” means a person or entity that 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 at issue.

“Subscriber Agreement” is the agreement executed between a Subscriber and the CA or Symantec relating to the provision of designated Certificate-related services governing the Subscriber’s rights and obligations relating to the Certificate. The STN Subscriber Agreement is published in the repository on the Symantec website.

“Symantec Managed PKI Service Description (February 2013)
laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such key pairs.

4. **SYMANTEC’S OBLIGATIONS**

   (a) **Services.** Following completion of the requisite installation, Symantec shall provide Customer with the services specified in this Service Description in accordance with these terms and conditions throughout the term of the service. Symantec shall issue, manage, revoke, and/or renew Certificates in accordance with the instructions provided by Customer and its Managed PKI Administrator(s). Symantec shall also register Public Keys, provide Public Keys to relying parties, and revoke the registration of Public Keys under XKMS in response to properly-structured XKMS requests submitted by Customer. Upon Customer’s approval of a Certificate Application, Symantec: (i) shall be entitled to rely upon the accuracy of the information in each such approved Certificate Application; and (ii) shall issue a Certificate for the Certificate Applicant for which such Certificate Application was submitted. Certificates issued or licensed under this Service Description, including Administrator Certificates, will have a maximum Operational Period of twelve (12) months from the date each Certificate is issued.

   (b) **Administrator Certificate.** Upon Customer’s submission of a Certificate Application for an Administrator Certificate and Symantec’s completion of authentication procedures required for the Administrator Certificate, Symantec will process the Certificate Application. Symantec will notify Customer whether Customer’s Certificate Application for an Administrator Certificate is approved or rejected. Managed PKI Administrator’s use of the PIN from Symantec to pick up the Administrator Certificate or otherwise installing or using the Administrator Certificate shall constitute Managed PKI Administrator’s acceptance of the Administrator Certificate. After the Managed PKI Administrator picks up or otherwise installs the Administrator Certificate, the Managed PKI Administrator must review the information in it before using it and promptly notify Symantec of any errors. Upon receipt of such notice, Symantec may revoke the Administrator Certificate and issue a corrected Administrator Certificate.

   (c) **CA Key Generation.** During a single CA Key Generation event, Symantec shall generate for Customer, pairs of CA keys for use in signing Certificates issued by Symantec on behalf of Customer for use in the STN. Customer CA Private Key of each key pair shall be stored in one or more Certificate Signing Units.

   (d) **Symantec’s Warranties.** Symantec warrants that: (i) there are no errors introduced by Symantec in the Certificate information as a result of Symantec’s failure to use reasonable care in creating the Certificate; (ii) its issuance of the Certificate(s) complies in all material respects with the STN CPS; and (iii) its revocation services and use of a repository conform to the STN CPS in all material aspects.

5. **ADDITIONAL TERMS**

   (a) **CA Certificate.** Each service account includes at least one CA Certificate. Additional CA Certificates for a given volume may be purchased later. Any extraction of CA Certificates and/or corresponding key pairs from Symantec systems and services will be subject to agreement of the parties.

   (b) **Administrator Kit.** Each Administrator Kit consists of a token, software and one (1) Administrator Certificate. Additional Administrator Kits for a given volume may be purchased later.
Symantec® Managed Public Key Infrastructure (PKI) service provides customers with the ability to issue certificates from a private Certificate Authority (CA). Symantec performs a formal, secure procedure to create private/public key pair for this CA called a key ceremony. These certificates are generally used to control access to organizational resources. For example, many customers only trust their private CA for their virtual private network (VPN) to prevent unauthorized access to their networks.

Every customer is automatically provisioned a private Certificate Authority (CA) as part of the standard package. This CA is based on the vetted customer’s legal entity name provided to Symantec for setting up the account. If a customer wants to use another name trademarked to that organization (e.g., a brand name versus a legal entity name) or change any of the default values in the CA, the customer may purchase an option to create additional CAs.

Note: Customers are responsible for defining and following their own Certification Practice Statement (CPS) that governs the issuing, managing, and use of certificates from the applicable private CA.

TERMS AND CONDITIONS FOR PRIVATE CERTIFICATE AUTHORITY

1. DEFINITIONS

“Administrator Certificate” means the Certificate issued by Symantec to the Customer employee or such other Trusted Person designated as the Managed PKI Administrator for the sole purpose of accessing the PKI Manager to perform Administrator functions.

“Agreement” means the Professional Services Agreement or such other master agreement entered into between Symantec and Customer under which the Services Order applicable to this Service Description is issued.

“Certificate” or “Digital Certificate” means a message that, at least, states a name or identifies the issuing CA, identifies the Subscriber, contains the Subscriber’s Public Key, identifies the Certificate’s Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing CA.

“Certificate Applicant” means a person or authorized agent that requests the issuance of a Certificate by a CA.

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

“Certificate Signing Unit” or “CSU” means a hardware unit or software designed for use in signing Certificates and key storage.

“Certification Authority” or “CA” means a person authorized to issue, suspend, or revoke Certificates.

“Erroneous Issuance” means: (a) issuance of a Certificate to a person other than the one named as the subject of the Certificate; or (b) issuance of a Certificate without the authorization of the person named as the subject of the Certificate.

“Key Generation” means the Symantec procedures for proper generation of Customer’s Public Key and Private Key via a trustworthy process and for storage of Customer’s Private Key and documentation thereof.

“Managed PKI Administrator” means an employee of the Registration Authority or such other Trusted Person authorized to perform RA tasks.

“Operational Period” means a 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 a date and time at which the Certificate expires or is earlier revoked.

“Private Hierarchy” means a domain consisting of a system of CAs that issue Certificates in a chain leading from Customer’s root CA through one or more Certification Authorities to Subscribers in accordance with Customer’s practices. Certificates issued in a Private Hierarchy are intended to meet the needs of organizations authorizing their issuance and are not intended for interactions between organizations and/or individuals through public channels.

“Private Key” means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.

“Public Key” means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.

“Registration Authority” or “RA” is an entity that performs identification and authentication of Certificate Applicants for Certificates, initiates or passes along revocation requests for Certificates, or approves applications for renewal or re-keying of Certificates. A RA is not an agent of a Certificate Applicant. A RA may not delegate the authority to approve Certificate Applications other than to authorized Managed PKI Administrators of the RA.

“Seat” means a single Subscriber that is an authorized end user of the service, without regard to the number of Certificates actually issued to that Subscriber.
“Subscriber” means a person or entity that 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 at issue.

“Subscriber Agreement” is the agreement executed between a Subscriber and the CA or Symantec relating to the provision of designated Certificate-related services and governing the Subscriber’s rights and obligations relating to the Certificate.

“Trusted Person” means an employee, contractor, or consultant of Customer who is responsible for managing infrastructural trustworthiness of Customer, its products, its services, its facilities, and/or its practices.

2. **CUSTOMER’S OBLIGATIONS**

   
   **(a) Appointment.** Customer shall appoint one or more authorized Customer employees or Trusted Persons as Managed PKI Administrator(s). Such Managed PKI Administrator(s) shall be entitled to appoint additional Managed PKI Administrators on Customer’s behalf. Customer shall cause Managed PKI Administrators receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement.

   **(b) Administrator Functions.** Customer shall, through its Managed PKI Administrator(s) using hardware and software designated by Symantec, validate the information in Certificate Applications, approve or reject such Certificate Applications, and instruct Symantec to issue, renew and revoke Certificates. If a Managed PKI Administrator ceases to have the authority to act as a Managed PKI Administrator on behalf of Customer, Customer shall promptly request revocation of the Administrator Certificate of such Managed PKI Administrator.

   **(c) Survival.** In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in these Service Terms and Conditions shall survive termination of the Agreement or the applicable Services Order until the end of the Operational Period of all Certificates issued hereunder.

   **(d) Customer’s Warranties.** In addition to the express limited warranties set forth in the Agreement, Customer warrants that (i) all information material to the issuance of a Certificate and validated by or on behalf of Customer is true and correct in all material respects; (ii) Customer’s approval of Certificate Applications will not result in Erroneous Issuance; (iii) no Certificate information provided to Symantec infringes the intellectual property rights of any third parties; (iv) information in the Certificate Application(s) (including email address(es)) has not been and will not be used for any unlawful purpose; (v) Customer’s Managed PKI Administrator has been (since the time of the Administrator Certificate’s creation) and will remain the only person possessing the Administrator Certificate Private Key, or any challenge phrase, PIN, software, or hardware mechanism protecting the Private Key, and no unauthorized person has had or will have access to such materials or information; (vi) Customer will use the Administrator Certificate exclusively for authorized and legal purposes consistent with this Service Description; (vii) Customer will not monitor, interfere with or reverse engineer the technical implementation of the Symantec systems or software or otherwise knowingly compromise the security of the Symantec systems or software.

   **(e) Compliance with Local Laws.** Customer is responsible for ensuring that Customer’s acquisition, use, or acceptance of public and private key pairs generated by Symantec in accordance with this Service Description complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such key pairs.

3. **SYMTEC’S OBLIGATIONS**

   **(a) Services.** Following completion of the requisite installation, Symantec shall provide Customer with the services specified in this Service Description in accordance with these terms and conditions throughout the term of the service. Symantec shall issue, manage, revoke, and/or renew Certificates in accordance with the instructions provided by Customer and its Managed PKI Administrators. Symantec shall also register Public Keys, provide Public Keys to relying parties, and revoke the registration of Public Keys under XKMS in response to properly-structured XKMS requests submitted by Customer. Upon Customer’s approval of a Certificate Application, Symantec: (i) shall be entitled to rely upon the accuracy of the information in each such approved Certificate Application; and (ii) shall issue a Certificate for the Certificate Applicant for which such Certificate Application was submitted. Certificates issued or licensed under this Service Description, including Administrator Certificates, will have a maximum Operational Period of twelve (12) months from the date each Certificate is issued.

   **(b) Administrator Certificate.** Upon Customer’s submission of a Certificate Application for an Administrator Certificate and Symantec’s completion of authentication procedures required for the Administrator Certificate, Symantec will process Customer’s Certificate Application. Symantec will notify Customer whether Customer’s Certificate Application for an Administrator Certificate is approved or rejected. Managed PKI Administrator’s use of the PIN from Symantec to pick up the Administrator Certificate or otherwise installing or using the Administrator Certificate shall constitute Managed PKI Administrator’s acceptance of the Administrator Certificate. After the Managed PKI Administrator picks up or otherwise installs the Administrator Certificate, the Managed PKI Administrator must review the information in it before using it and promptly notify Symantec of any errors. Upon receipt of such notice, Symantec may revoke the Administrator Certificate and issue a corrected Administrator Certificate.

   **(c) CA Key Generation.** During a single CA Key Generation event, Symantec shall generate for Customer pairs of CA keys for use in signing Certificates issued by Symantec on behalf of Customer for use in Customer’s Private Hierarchy. Customer’s Private Key of each pair shall be stored in one or more Certificate Signing Units.

   **(d) Symantec’s Warranty.** Symantec warrants that there are no errors introduced by Symantec in the Certificate information as a result of Symantec’s failure to use reasonable care in creating the Certificate.

4. **ADDITIONAL TERMS**
(a) **CA Certificate.** Each service account includes at least one CA Certificate. Additional CA Certificates for a given volume may be purchased later. Any extraction of CA Certificates and/or corresponding key pairs from Symantec systems and services will be subject to agreement of the parties.

(b) **Administrator Kit.** Each Administrator Kit consists of a token, software and one (1) Administrator Certificate. Additional Administrator Kits for a given volume may be purchased later.
Symantec™ Managed Public Key Infrastructure (PKI) service provides customers with the ability to issue certificates from Adobe® Certified Document Services (CDS). Symantec has worked with Adobe to have ability to issue certificates automatically trusted by Adobe Acrobat®, Reader®, and LiveCycle® products. These certificates are used to digitally sign portable document files (PDF) in these products.

Every customer is automatically provisioned an issuing Certificate Authority (CA) chaining to Symantec Intermediate CA for Adobe CDS as part of standard package. This CA is based on the vetted customer’s legal entity name provided to Symantec for setting up the account. If a customer wants to use another name trademarked to that organization (e.g., a brand name versus a legal entity name) or change any of the default values in the CA, the customer may purchase an option to create additional CAs.

Note: Customers and user must adhere to the Adobe CDS Certification Practice Statement (CPS) to issue, manage, and use these certificates.

**TERMS AND CONDITIONS FOR ADOBE CDS**

1. **DEFINITIONS**
   “Administrator Certificate” means the Certificate issued by Symantec to the Customer employee or such other Trusted Person designated as the Managed PKI Administrator for the sole purpose of accessing the PKI Manager to perform Administrator functions.
   “Agreement” means the Professional Services Agreement or such other master agreement entered into between Symantec and Customer under which the Service Order applicable to this Service Description is issued.
   “Certificate” or “Digital Certificate” means a message that, at least, states a name or identifies the issuing CA, identifies the Subscriber, contains the Subscriber’s Public Key, identifies the Certificate’s Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing CA.
   “Certificate Applicant” means a person or authorized agent that requests the issuance of a Certificate by a CA.
   “Certificate Application(s)” means a request from a Certificate Applicant (or authorized agent) to a CA for the issuance of a Certificate.
   “Certification Practices Statement” or “CPS” means a document, as revised from time to time, representing a statement of the practices a CA or RA employs in issuing Certificates. For purposes of this Managed PKI for Adobe® CDS Service Description, “CPS” shall mean the Symantec – Adobe Certified Document Service (CDS) PKI Certification Practice Statement, published in the repository on the Symantec website. “Certificate Signing Unit” or “CSU” means a hardware unit or software designed for use in signing Certificates and key storage.
   “Certification Authority” or “CA” means a person authorized to issue, suspend, or revoke Certificates.
   “Erroneous Issuance” means (a) issuance of a Certificate in a manner not materially in accordance with the procedures required by the CPS; (b) issuance of a Certificate to a person other than the one named as the subject of the Certificate; or (c) issuance of a Certificate without the authorization of the person named as the subject of the Certificate.
   “Key Generation” means the Symantec procedures for proper generation of Customer’s Public Key and Private Key via a trustworthy process and for storage of Customer’s Private Key and documentation thereof.
   “Managed PKI Administrator” means an employee of the Registration Authority or such other Trusted Person authorized to perform RA tasks.
   “Operational Period” means a 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 a date and time at which the Certificate expires or is earlier revoked.
   “Private Hierarchy” means a Certification Authority to issue Certificates in a hierarchy other than STN. In the context of Adobe CDS, the Certificate Authority chains to the Symantec Intermediate CA for Adobe CDS, which, in turn, chains to the Adobe Root CA.
   “Private Key” means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.
   “Public Key” means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.
   “Registration Authority” or “RA” is an entity that performs identification and authentication of Certificate Applicants for Certificates, initiates or passes along revocation requests for Certificates, or approves applications for renewal or re-keying of Certificates. A RA is not an agent of a Certificate Applicant. A RA may not delegate the authority to approve Certificate Applications other than to authorized Managed PKI Administrators of the RA.
“Seat” means a single Subscriber that is an authorized end user of the service, without regard to the number of Certificates actually issued to that Subscriber.

“Subscriber” means a person or entity that 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 at issue.

“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.

“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 Symantec and its affiliates, and their respective customers, subscribers, and relying parties.

“Trusted Person” means an employee, contractor, or consultant of Customer who is responsible for managing infrastructural trustworthiness of Customer, its products, its facilities, and/or its practices.

2. CUSTOMER’S OBLIGATIONS

   (a) Appointment. Customer shall appoint one or more authorized Customer employees or Trusted Persons as Managed PKI Administrator(s). Such Managed PKI Administrator(s) shall be entitled to appoint additional Managed PKI Administrators on Customer’s behalf. Customer shall cause Managed PKI Administrators receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement and the CPS.

   (b) Administrator Functions. Customer shall, through its Managed PKI Administrator(s) using hardware and software designated by Symantec, validate the information in Certificate Applications, approve or reject such Certificate Applications, and instruct Symantec to issue, renew and revoke Certificates in accordance with the CPS, published at the PKI Manager and amended from time to time. If a Managed PKI Administrator ceases to have the authority to act as a Managed PKI Administrator on behalf of Customer, Customer shall promptly request revocation of the Administrator Certificate of such Managed PKI Administrator.

   (c) Survival. In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in these Service Terms and Conditions and the CPS, shall survive termination of the Agreement or the applicable Services Order until the end of the Operational Period of all Certificates issued hereunder.

   (d) Customer’s Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants that (i) all information material to the issuance of a Certificate and validated by or on behalf of Customer is true and correct in all material respects; (ii) Customer’s approval of Certificate Applications will not result in Erroneous Issuance; (iii) Customer has substantially complied with the CPS; (iv) no Certificate information provided to Symantec infringes the intellectual property rights of any third parties; (v) information in the Certificate Application(s) (including email address(es)) has not been and will not be used for any unlawful purpose; (vi) Customer’s Managed PKI Administrator has been (since the time of the Administrator Certificate’s creation) and will remain the only person possessing the Administrator Certificate Private Key, or any challenge phrase, PIN, software, or hardware mechanism protecting the Private Key, and no unauthorized person has had or will have access to such materials or information; (vii) Customer will use the Administrator Certificate exclusively for authorized and legal purposes consistent with this Service Description; (viii) Customer will not monitor, interfere with or reverse engineer the technical implementation of the Symantec systems or software or otherwise knowingly compromise the security of the Symantec systems or software.

   (e) Customer’s Subscribers. Customer shall cause Subscribers receiving Certificates hereunder to abide by the terms of the appropriate Subscriber Agreement, to which they shall assent as a condition of enrolling for their Certificates. Customer will ensure that the terms of such Subscriber Agreement shall be no less protective of CAs than those in the CPS.

   (f) Compliance with Local Laws. Customer is responsible for ensuring that Customer’s acquisition, use, or acceptance of public and private key pairs generated by Symantec in accordance with this Service Description complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such key pairs.

3. SYMANTEC’S OBLIGATIONS

   (a) Services. Following completion of the requisite installation, Symantec shall provide Customer with the services specified in this Service Description in accordance with these terms and conditions throughout the term of the service. Symantec shall issue, manage, revoke, and/or renew Certificates in accordance with the instructions provided by Customer and its Managed PKI Administrator. Symantec shall also register Public Keys, provide Public Keys to relying parties, and revoke the registration of Public Keys under XKMS in response to properly-structured XKMS requests submitted by Customer. Upon Customer’s approval of a Certificate Application, Symantec (i) shall be entitled to rely upon the accuracy of the information in each such approved Certificate Application; and (ii) shall issue a Certificate for the Certificate Applicant for which such Certificate Application was submitted. Certificates issued or licensed under this Service Description, including Administrator Certificates, will have a maximum Operational Period of twelve (12) months from the date each Certificate is issued.

   (b) Administrator Certificate. Upon Customer’s submission of a Certificate Application for an Administrator Certificate and Symantec’s completion of authentication procedures required for the Administrator Certificate, Symantec will process the Certificate Application. Symantec will notify Customer whether Customer’s Certificate Application for an Administrator Certificate is approved or rejected. Managed PKI Administrator’s use of the PIN from Symantec to pick up the Administrator Certificate or otherwise installing or using the Administrator Certificate shall constitute Managed PKI Administrator’s acceptance of the Administrator Certificate. After the Managed PKI Administrator picks up or otherwise installs
the Administrator Certificate, the Managed PKI Administrator must review the information in it before using it and promptly notify Symantec of any errors. Upon receipt of such notice, Symantec may revoke the Administrator Certificate and issue a corrected Administrator Certificate.

(c) **CA Key Generation.** If required, Symantec shall generate for Customer pairs of CA keys for use in signing Certificates issued by Symantec on behalf of Customer during a single CA Key Generation event. Customer’s Private Key of each pair shall be stored in one or more Certificate Signing Units.

(d) **Symantec’s Warranty.** Symantec warrants that there are no errors introduced by Symantec in the Certificate information as a result of Symantec’s failure to use reasonable care in creating the Certificate.

4. **ADDITIONAL TERMS OF SERVICE**

(a) **CA Certificate.** Each service account includes at least one CA Certificate. Additional CA Certificates for a given volume may be purchased later. Any extraction of CA Certificates and/or corresponding key pairs from Symantec systems and services will be subject to agreement of the parties.

(b) **Administrator Kit.** Each Administrator Kit consists of a token, software and one (1) Administrator Certificate. Additional Administrator Kits for a given volume may be purchased later.
Appendix D: LTE Certificate Service

Symantec's LTE Service ("LTES" or "Service") provides customer with an ability to obtain device Certificates in a private hierarchy for integration into operator LTE equipment. Customer or their Operators submits request to Symantec for LTE through a programmatic interface such as the Certificate Management Protocol (CMP).

1. DEFINITIONS

"Administrator Certificate" means the client Certificate issued by Symantec to a Customer appointed Service Administrator or such other Trusted Person designated as the Managed PKI Administrator for the purpose of accessing Web Portal to manage LTE end entity Certificates

"Affiliated Individual" means a person that is affiliated to Customer: (a) as an officer, director, employee, partner, contractor, intern, or other person within Customer’s organization; or (b) as a person maintaining a contractual relationship with Customer’s organization where Customer has business records providing strong assurances of the identity of such person.

"Agreement" means the Professional Services Agreement or such other master agreement entered into between Symantec and Customer under which the Services Order applicable to this Service Description is issued.

"Certification Authority" or “CA” means a person or entity authorized to issue, suspend, or revoke Certificates.

"Certificate Management Protocol" or “CMP” means a protocol for auto-enrollment and lifecycle management of the device certificates. Devices will interface directly with Symantec PKI System via CMP. The devices have to be pre-authorized by an Administrator before the device is permitted to send CMP request to the PKI System.

"Operational Period" means a period starting with the date and time a Certificate is issued and ending at the date and time at which the Certificate expires.

"Operator" means a business entity that is a subsidiary of the Customer typically from another country or region and is treated as a Sub-account of the Customer by Symantec

"LTE Certificate" means a message to be stored in a device, including a name, the issuing CA, or a network element in the operator network. The network element may be an Operator Base Station or a Security Gateway or other similar device. In all cases, the LTE Certificate contains the network element’s Public Key, Certificate’s Operational Period, a Certificate serial number, and a digital signature of the issuing CA.

"Private Hierarchy" means a domain consisting of a system of CAs that issue LTE Certificates in a chain leading from Customer’s Root CA through one or more Certification Authorities to Subscribers in accordance with Customer’s practices. Certificates issued in a Private Hierarchy are intended to meet the needs of organizations authorizing their issuance and are not intended for interactions between organizations and/or individuals through public channels.

"Private Key" means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.

"Public Key" means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.

"Root CA" means the top entity in the domain of trusted hierarchy and Root CA is identified by a "Root Certificate".

"Service Administrator" means a trusted employee of Customer or Affiliate that has been designated to perform certain Certificate related administrative functions described in the Service Description.

"Subscriber" means a person or entity that 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 at issue.

"Subscriber Agreement" is the agreement executed between a Subscriber and the CA or Symantec relating to the provision of designated Certificate-related services and governing the Subscriber’s rights and obligations relating to the Certificate.

"Vendor" or “Manufacturer” (sometimes used interchangeably) means a business entity that has provided the network element to the Operator.

"Web Portal" means the Symantec hosted web interface accessible by Service Administrators for the purpose of requesting LTE Certificate

2. CUSTOMER’S OBLIGATION

(a) Appointment. Customer shall appoint one or more authorized Customer and/or Operator employees as Service Administrators for the entities employing such personnel. Customer shall require Service Administrators receiving Administrator Certificates hereunder to abide by the terms of the applicable Subscriber Agreement associated with such Certificates, and to use Service Administrator Certificates exclusively for authorized and legal purposes consistent with this Service Description. Customer must immediately request revocation of the applicable Administrator Certificate if the subscriber ceases to be an authorized Service Administrator.

(b) Administrator Functions. Customer and/or its Operators, as applicable, through the appointed Service Administrators, shall be responsible for:

i. creation of operator sub-account,
ii. creation of certificate profiles,
iii. provide vendor CA certificates,
iv. provide IP address blocks for validation,
v. register new devices and set up a pre-approval for a future request, and
vi. configure CMP responder URL to on network elements

(c) Account Authorization. Customer shall provide Symantec advance written authorization of any Operator authorized to receive LTE Certificate issued hereunder, including such Operator’s contact information, identification of the individual(s) designated to be Service Administrator(s) for such Operator (including enrollment information therefore), and the number of LTE Certificates and sites for which each Operator has been authorized. Customer shall ensure, and require its Operator(s) to ensure, that each Service Administrator has been (since the time of the applicable Service Administrator Certificate’s creation) and will remain the only person possessing such Certificate’s Private Key, any challenge phrase, PIN, software, or hardware mechanism protecting the Private Key, and no unauthorized person has had or will have access to aforementioned material or information.

(d) Other Obligations. Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system or software, and will impose the same restriction on its appointed Vendors or Manufacturers.

(e) Survival. In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in this Service Description shall survive termination of the Agreement or the applicable Services Order until the end of the Operational Period of all Certificates issued hereunder.

(f) Compliance with Local Laws. Customer is responsible for ensuring that Customer’s acquisition, use, or acceptance of public and private key pairs generated by Symantec in accordance with this Service Description complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such key pairs.

3. SYMANTEC’S OBLIGATIONS

(a) Service Administrator Certificates. Upon Symantec's successful completion of validation procedures required for an Administrator Certificate requested by Customer, Symantec will provide such Administrator Certificate to the applicable Service Administrator. A Service Administrator's use of a PIN from Symantec to pick up the Administrator Certificate or otherwise installing or using the Administrator Certificate is considered acceptance of the Administrator Certificate. After the Service Administrator picks up or otherwise installs the Administrator Certificate, the Service Administrator must review the information in the Administrator Certificate before using it and promptly notify Symantec of any errors. Upon receipt of any such notice, Symantec may revoke the Administrator Certificate and issue a corrected Administrator Certificate.

(b) Service Structure. Symantec will create and host, in accordance with Symantec’s standard PKI practices and policies, two (2) Customer Root Certificates and optionally up to two (2) CA Certificates issued under each root Certificate, which CA Certificates will be used solely for the purpose of providing the Service to Customer hereunder. Additional CA Certificates may be purchased separately. Symantec will onboard Operators and create sub-accounts for them based on requests from the Customer with accordance with standard PKI practices and policies.

(c) IP address configuration. As part of the on-boarding process of a new Operator, a range of valid IP addresses is provided to Symantec. Symantec's System shall only respond to CMP requests coming from the valid IP addresses and all other requests not originated from the configured IP addresses are rejected. This configuration will need to be performed by the Operator.

(d) Services. Upon a Service Administrator’s submission through the Web Portal of a Certificate request for which the requested number of Certificates have been authorized by Customer pursuant to Section 2(d) of this Service Description, Symantec shall be entitled to (i) rely upon the accuracy of the information in each such Certificate request, and (ii) issue and provide such Certificates to the requesting Service Administrator. Device Certificates issued or licensed under this Service Description (i) will have a validity period of one (1), two (2) or three (3) years from the date the Certificate was issued, and (ii) may not be integrated with or installed in any device that does not correspond to the applicable Certificate request. Symantec will fulfill all orders meeting the forgoing requirements in the order received. Notwithstanding any inconsistent provision hereof, the number of Operators that may request Certificates, and the number production sites and Service Administrators through which Certificates may be requested, will be strictly limited to the number specified in the applicable Service Order(s).

(e) Account Activation. Subject to advance purchase through a Services Order, Symantec shall use commercially reasonable efforts to activate sub-accounts based within the United States within ten (10) business days and accounts outside of the United States within a commercially reasonable period upon the following requirements being satisfied: (i) completion of the necessary enrollment process; and (ii) authentication of the Operator and its Service Administrator(s) (the Service Administrator(s) must be accessible during this period in order for Symantec to perform authentication in a timely manner)

(f) Symantec’s Warranties. Symantec warrants that there are no errors introduced by Symantec in the Certificates issued hereunder as a result of Symantec's failure to use reasonable care in creating the Certificates.

(g) Audit Rights. Symantec may conduct an audit of Customer’s procedures not more than once per year to ensure compliance with the terms of this Service Description. Any such audit will be conducted during business hours upon reasonable
written notice to Customer and will not unreasonably interfere with Customer’s business activities. Customer shall reasonably cooperate with Symantec in connection with any such audit. If the audit reveals that Customer has breached any term of these Service Description Terms and Conditions, then: (i) Customer will pay Symantec’s reasonable costs of conducting the audit, and (ii) notwithstanding the one audit per year limitation stated above, Symantec may conduct such further audits as it deems reasonably necessary to ensure compliance with the terms herein. Routine annual audits may only cover the activities of the immediately preceding year.