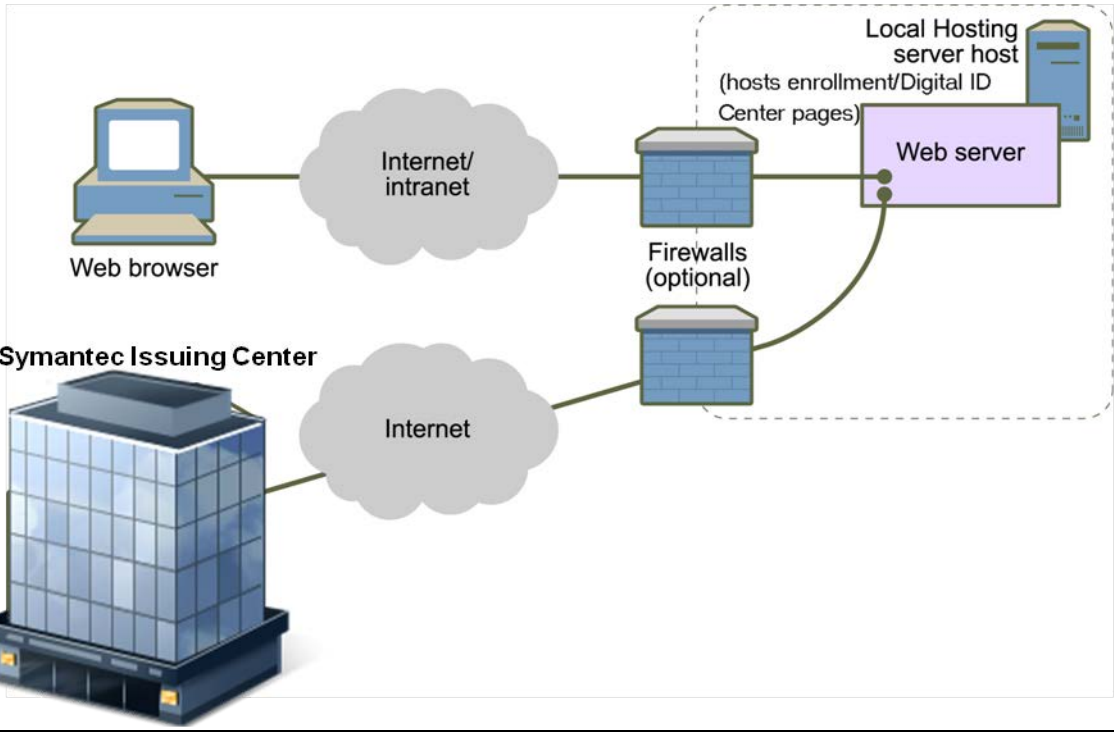
Symantec Managed PKI Certificate Service Description (< version 8.0)

Introduction
Symantec Managed PKI Service provides an integrated PKI platform for you by combining enterprise controlled and operated PKI software and hardware, compatibility with popular applications, and Symantec's certificate processing services and infrastructure.

To implement your own PKI solution, you would need to set up systems, telecommunications, databases, physical site security, Internet-safe network configurations, high-availability redundant systems, disaster recovery, viable PKI legal practices, and hire PKI specialists. Managed PKI Service provides this infrastructure for you, operating on Symantec's highly-available and highly-secure PKI back end, thus enabling your organization to reap the benefits of PKI without the risk, effort and expense of buying and maintaining your own PKI system. Managed PKI Service supports your enterprise globally, enabling your users to enroll for digital certificates and view digital certificate content in major Asian and European languages.

Diagram 1 – Typical Local Hosting Configuration
Note: Equipment within the dotted box resides at your site



Core Features

- *Managed PKI Digital ID Center*
  You may choose to have Symantec or your organization host the Digital ID Center pages for end-user certificate enrollment. With **Symantec hosting**, the Digital ID Center pages are hosted at the Symantec™ Issuing Center whereas with **Local Hosting** (see **Diagram 1**), your organization maintains the Digital ID Center pages on your own web server. Certificates are issued by Symantec regardless of where these pages are hosted. Local hosting enables your organization to customize and co-brand the Digital ID Center pages with your own text, links, and/or logo. Local hosting is required to implement Automated Administration, and Outsourced Authentication services.

- *Managed PKI Control Center*
  Management of the lifecycle process for enrolling, approving, revoking and renewing certificates is performed through the Managed PKI Control Center, which gives your organization full control over the registration and authentication process. Your organization may appoint an unlimited number of Managed PKI administrators, which provides for a separation of duties. Managed PKI Service administrators ensure that Digital IDs are issued only to properly authenticated individuals or entities in accordance with the practices of your organization. Administrators review certificate requests and approve them or reject them. Administrators download certificate revocation lists (CRLs), lists of certificates that have been revoked, to ensure that invalid certificates are not accepted by the system. Administrators also generate reports and monitor the operation of Managed PKI Service, as well as instruct users in the usage of their Digital IDs. The Managed PKI Control Center resides within Symantec's Data Center.

- *Symantec™ Issuing Center*
  The Symantec Issuing Center is responsible for processing requests for new certificates or renewals. Once a request is approved by your Managed PKI Service administrator, the Issuing Center issues the certificate, and then sends the applicant an email notification to retrieve the certificate. The Issuing Center also generates reports and certificate revocation lists (CRLs), which are used by your Managed PKI Service administrators to manage your Managed PKI Service customer accounts. The Issuing Center resides within Symantec's Data Center.

- *Authentication Methods*
  Symantec Managed PKI Service offers several methods for authenticating and approving requests: Manual Authentication, Passcode Authentication and Automated Administration.

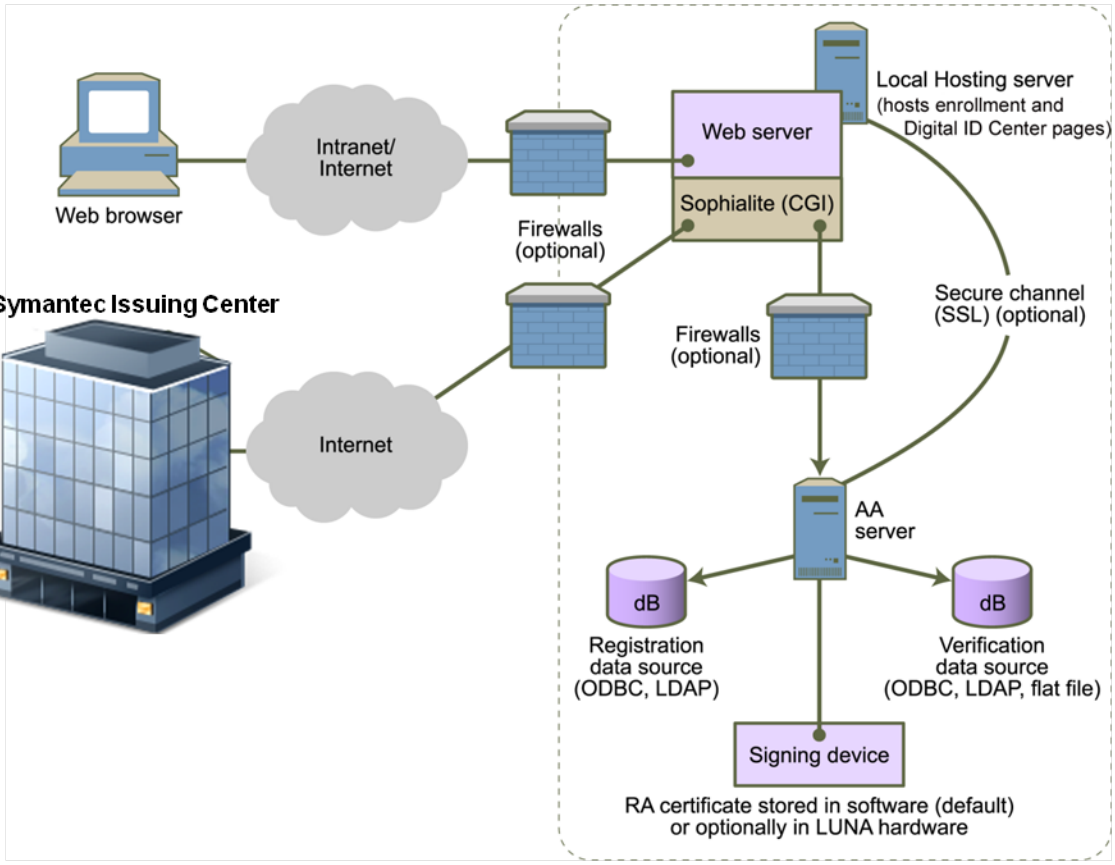
  Manual Authentication
  With Manual Authentication, the administrator personally reviews and approves or rejects each certificate request. Due to the time required of administrators, manual authentication may not be suitable for organizations that issue a high volume of certificates.

  Passcode Authentication
  Passcode Authentication is a service that automatically authenticates certificate requests. The administrator configures Passcode Authentication through the Managed PKI Control Center. When a subscriber applies for a certificate, the enrollment information is securely uploaded to Symantec and compared to information previously provided by the administrator. Depending upon approval guidelines established by your organization, the certificate request is either approved or rejected. Unlike Automated Administration, Passcode Authentication does not require your organization to establish and maintain authentication servers. Instead, all authentication is performed at Symantec based on the subscriber data uploaded by the administrator. As a result, Passcode Authentication is easier to implement but slightly less flexible than Automated Administration.

  Automated Administration
  With the Automated Administration (AA) option, Managed PKI Service automatically processes certificate applications without administrator assistance at the time of enrollment. See **Diagram 2**. Automated Administration compares the enrollment data provided by the certificate applicant with data from your source (such as your Human Resources database or an LDAP directory). If the applicant is authenticated (that is, if the data matches), then the request is approved. With the Automated Administration API, your software can automatically add data to the approved request. Upon receipt of the request, Symantec adds the information to the new certificate. Thus, you may customize and automate the certificate authentication and issuing process. The Automated Administration server resides at your site.

  Diagram 2 – Typical Automated Administration Configuration
  Note: Equipment within the dotted box resides at your site. For the purposes of the diagram below, the following definitions shall apply: RA – Registration Authority; LUNA hardware – certificate signing hardware; LDAP – Lightweight Directory Access Protocol; ODBC – Open

Database Connectivity; Sophialite (CGI) – Symantec™ common gateway interface program that accepts subscriber enrollment data from the locally hosted certificate enrollment pages.



Additional Options

The following options are available at additional charge:

- *Premium Validation Services*. Symantec provides certificate revocation in several forms:

  - *Real-Time Validation Service*
    Real-Time Validation Service – OCSP/XKMS enables you to validate certificates through Online Certificate Status Protocol (OCSP) or XML Key Management Specification (XKMS). An application may automatically recognize the revocation status of a certificate. Revocation statuses include *valid*, *revoked*, *suspended*, *expired* or *unknown*. For OCSP, when a user presents a certificate to a web server or other network resource, CVM (Certificate Validation Module) requests the certificate status from the Certification Authority (CA). For XKMS, your application integrates the XKMS client, which requests certificate status from the CA.

  - *Premium CRL Service*
    With Premium CRL Service, Symantec updates CRLs hourly rather than daily. When a user presents a certificate to a web server or other network resource, an application may check the certificate against the CRL. If the certificate is listed as *revoked*, the user cannot access the resource. If the certificate is not listed, the user will be able to access the resource.

- *Key Management Service*. Managed PKI Service allows for centralized key generation, private key backup and distributed key recovery to ensure maximum security and protection of private keys. Dual key

pair generation is also supported, which allows for separate issuance and backup of encryption and signing key pairs.

Public Certification

Public certificates reside in the Symantec™ Trust Network (STN), a globally-interoperable digital certificate infrastructure based on a trusted network of Certification Authorities throughout the world. The roots of the Symantec™ Trust Network are embedded in all popular browsers, servers, and email applications. Therefore, public certificates can be used across organizations without any special preparation on the part of the certificate users. Because Symantec Managed PKI Co-Branded Certificate Service is provided under a public CA, your organization must adhere to the Symantec™ Certification Practice Statement (CPS).

Private Certification

When your organization enrolls for the Symantec Managed PKI Private Label Service, Symantec will perform a key ceremony for you: a formal, secure procedure for creating the private/public key pair for your CA with your own private root at the top of the CA hierarchy. Generally, private certificates are used within your organization for applications such as intranets, virtual private networks (VPNs), and, occasionally, for Web access. Although private certificates may be used externally in private domains, you must first distribute your organization's root and certificates to those with whom you wish to communicate. Organizations running a private CA are responsible for defining and following their own certificate rules and practices.

Note: IPSec implementations for VPNs require use of private certification.

APPENDIX A – MPKI CO-BRANDED CERTIFICATES SERVICE TERMS AND CONDITIONS

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 Managed PKI Control Center 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.

"Trusted Person" has the meaning given in the CPS.

"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.

2. APPOINTMENT

(a) Appointment. Symantec hereby appoints Customer as a non-Symantec CA within the STN pursuant to the STN CPS, and Customer accepts such appointment.

(b) STN CPS. Except for the functions outsourced to Symantec under this Service Description, Customer shall meet all requirements and perform all obligations imposed upon a CA and/or RA within the STN including but not limited to: (i) the STN CPS, as periodically amended; and (ii) the duties in Section 4 of these terms and conditions. Symantec shall notify the Customer-appointed Registration Authority Administrator of any amendments by posting the information to the Managed PKI Control Center.

3. CUSTOMER'S OBLIGATION

(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 CPS.

(b) Administrator Functions. Customer shall comply with the requirements stated in the STN CPS including without limitation, requirements for validating the information in Certificate Applications, approving or rejecting such Certificate Applications, and revoking Certificates, using hardware and software designated by Symantec. Customer shall perform such tasks in a competent, professional, and workmanlike manner. Customer shall approve a Certificate Application only if the Certificate Applicant is an Affiliated Individual as to Customer. If a Subscriber, who had been issued a Certificate by Customer, ceases to be affiliated with Customer as an Affiliated Individual, then Customer shall promptly request revocation of such Subscriber's Certificate through the Managed PKI Control Center. If a Managed PKI Administrator ceases to have the authority to act as Managed PKI Administrator on behalf of Customer, then Customer shall promptly request revocation of the Administrator Certificate of such Managed PKI Administrator.

(c) 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 STN CPS.

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

(e) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants to Symantec 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 RA requirements in the CPS; (iv) Certificate information provided to Symantec shall not infringe the intellectual property rights of any third party; (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'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 such material or information; (vii) Customer will use the Administrator Certificate exclusively for authorized and legal purposes consistent with this Agreement; and (viii) Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system, software or the STN.

(f) 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 herein 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.

(g) 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.

4. SYMANTEC'S OBLIGATIONS

(a) Services. Following completion of the requisite installation, Symantec shall provide Customer with the services specified in this Service Description 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 Agreement, 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.

APPENDIX B – MPKI PRIVATE LABEL CERTIFICATE SERVICE TERMS AND CONDITIONS

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 Managed PKI Control Center 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.

"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 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. 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 terms and conditions and the CPS shall survive termination of this Agreement 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 its 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 Agreement; (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) 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 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 Agreement, 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.

APPENDIX C –ADOBE CERTIFIED DOCUMENT SERVICES TERMS AND CONDITIONS

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 Managed PKI Control Center 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.

"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 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 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 Managed PKI Control Center 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 the CPS shall survive termination of this Agreement 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 Agreement; (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 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 Agreement, 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 – KEY MANAGEMENT SERVICE TERMS AND CONDITIONS:

1. DEFINITIONS

"Erroneous Key Recovery" means: (a) recovery and transmission of a Private Key in a manner not materially in accordance with the procedures required in the applicable CPS; (b) recovery and transmission of a Private Key to a person other than the Subscriber who is the rightful holder of the Private Key; or (c) recovery and transmission of a Private Key without the authorization of the Subscriber who is the rightful holder of the Private Key. Notwithstanding the foregoing, Erroneous Key Recovery does not include: (d) Customer's recovery of a Subscriber's Private Key and transmission to law enforcement officials in response to a search warrant or subpoena; (e) Customer's recovery of a Subscriber's Private Key and transmission in response to judicial or administrative process; or (f) Customer's recovery of a Subscriber's Private Key to obtain access to messages that are intended to be decrypted by use of such Private Key, even without Subscriber's authorization, for Customer's legitimate and lawful business purposes.

"Key Manager Administrator" means a person designated by Customer that shall use trustworthy systems to generate key pairs, send Public Keys and Private Key recovery information to Symantec, store Private Keys, and transmit Private Keys to Subscribers.

"Key Recovery Impersonation" means a request and receipt from Customer of a Subscriber's Private Key by submitting false or falsified information relating to naming or identity indicating that such Person is such Subscriber.

KMS.2. CUSTOMER'S OBLIGATIONS

(a) Appointment. Customer shall appoint one or more authorized Customer employees or such other Trusted Persons as Key Manager Administrators ("KMAs"). KMAs may have different roles, such as a security administrator role or a key recovery role. Only KMAs with a security administrator role shall be entitled to appoint additional KMAs on Customer's behalf. If any KMA is no longer authorized to recover keys, Customer shall use the Managed PKI Control Center to revoke such authority. Customer must comply with the applicable requirements of the Key Management Service Administrator's Guide published at the Managed PKI Control Center, as periodically amended. Symantec shall notify the Customer-appointed KMA of any such amendments by posting the information to the Managed PKI Control Center.

(b) Administrator Functions. Customer shall comply with the requirements of the Key Management Service Administrator's Guide including, without limitation, requirements for generating key pairs on behalf of Certificate Applicants, transmitting Public Keys to Symantec for inclusion in Certificates to be issued to such Certificate Applicants, transmitting key recovery information to Symantec, validating requests from Subscribers who wish to recover their Private Keys to ensure that they are in fact from such Subscribers, approving or rejecting such requests, using hardware and software designated by Symantec, using the Unified Authentication Managed PKI Key Management Service to request the information needed to recover Private Keys, and (where appropriate) transmitting recovered Private Keys to the requesting Subscribers. Customer shall use trustworthy systems to generate key pairs, send Public Keys and Private Key recovery information to Symantec, store Private Keys, and transmit Private Keys to Subscribers.

(c) Manner of Performance. Customer shall perform the tasks in Section KMS.2(b) above in a competent, professional, and workmanlike manner. Customer shall utilize Symantec's software and services provided under this Service Description exclusively for lawful purposes and for purposes consistent with the Key Management Service Administrator's Guide.

(d) Customer's Warranties. In addition to the express limited warranties contained in each applicable Service Description under this Agreement, Customer warrants that (i) each request by Customer to recover a Subscriber's Private Key has in fact been submitted to Customer and authorized by such Subscriber; (ii) requests by Customer to recover a Subscriber's Private Key without the Subscriber's permission are authorized by Customer for its legitimate and lawful business purposes; (iii) without limiting the generality of the foregoing, a request by Customer to recover a Subscriber's Private Key will not result in an Erroneous Key Recovery regardless of whether it results from Key Recovery Impersonation; and (iv) Customer has substantially complied with the Key Management Service Administrator's Guide.

(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

KMS.3. SYMANTEC'S OBLIGATIONS

Symantec shall provide the Key Management Service as set forth herein, to be used concurrently with the Symantec Managed PKI Service for Windows.

(a) KMA Certificate. Upon approval of a Certificate Application of the KMA(s), if any, Symantec shall issue a KMA Certificate or Administrator Certificate to each such KMA as appropriate to gain access to the services provided under this Service Description.

(b) Placement of Public Keys in Certificates. After Customer generates a key pair on behalf of a Certificate Applicant (upon approval of a Certificate Application) and transmits the Public Key to Symantec, Symantec shall place such Public Key in a Certificate and issue the Certificate pursuant to the applicable Symantec Managed PKI Service for Windows service terms.

(c) Symantec Centralized Key Management Service. Symantec shall authenticate requests received from Customer's KMA for a Subscriber's Private Key that Customer generated or approved in accordance with the Key Management Service Administrator's Guide. If Symantec authenticates the request, it shall provide

Customer with Key Recovery information needed to recover such Subscriber's Private Key.

KMS.4. LIABILITY RELATING TO REQUESTS FOR PRIVATE KEYS

CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR THE GENERATION OR AUTHENTICATION OF ALL RECOVERY REQUESTS FOR PRIVATE KEYS THAT CUSTOMER SUBMITS TO SYMANTEC AND FOR THE CONDUCT OF CUSTOMER'S KMAs. SYMANTEC DISCLAIMS ANY AND ALL LIABILITY ASSOCIATED THEREWITH.