Symantec™ Custom Device Certificate Service Description

Introduction
Customer wishes to use the Symantec™ Custom Device Certificate Service ("CDCS" or "Service") to obtain device Certificates in a private hierarchy for integration into certain hardware devices, based on batch Certificate signing requests submitted to Symantec by Customer or its manufacturers through a Symantec hosted Service console.

TERMS AND CONDITIONS

1. DEFINITIONS

"Administrator Certificate" means the client Certificate issued by Symantec to a Customer appointed Service Administrator for the sole purpose of accessing the Service Console to request CDCS end entity device Certificates.
"Administrator Kit" means a kit consisting of a USB token and extension cable, or an alternate strong two-factor authentication device, any associated software, and one year of maintenance and support for such kit.
"Agreement" means the Master Services Agreement entered into between Symantec and Customer under which the Service Order appended 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. For purposes of this Service Order, these terms will be deemed to refer to CDCS end entity device Certificates unless otherwise stated.
"Certification Authority" or **"CA"** means a person or entity authorized to issue, suspend, or revoke Certificates.
"Manufacturer" means a business entity (i) that Customer has authorized to receive Certificates issued hereunder, and (ii) for which there is in full force and effect a duly executed Digital Certificate agreement between Customer and such entity. Such business entity may, by way of example and without limitation, be manufacturing any device authorized by Customer to receive a Digital Certificate.
"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.
"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.
"CDCS Customer CA" the Digital Certificate, signed by a Symantec™ CDCS root Certificate, that is used to issue end entity device Certificates for Customer as further described in this Agreement.
"Service Administrator" means a trusted employee of Customer or a Manufacturer that has been designated to perform certain Certificate related administrative functions described in the Service Description.
"Service Console" means the Symantec hosted web interface accessible by Service Administrators for the purpose or requesting device Certificates.

2. CUSTOMER'S OBLIGATION

(a) Appointment. Customer shall appoint one or more authorized Customer and/or Manufacturer 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 Agreement. Customer must immediately request revocation of the applicable Administrator Certificate if the subscriber ceases to be an authorized Service Administrator. Customer must purchase one Administrator Kit for each Service Administrator.

(b) Administrator Functions. Customer and/or its Manufacturers, as applicable, through the appointed Service Administrators, shall be responsible for validating the information in device Certificate requests, submitting device Certificate requests through the Service Console, and integrating device Certificates into the corresponding devices identified in such Certificate requests. Customer will ensure, and will require its Manufacturer(s) to ensure, that all information material to the issuance of a Certificate and validated by or on behalf of Customer or such Manufacturer(s) (as applicable) is true and correct in all material respects.

(c) Relationship of Parties. The Parties agree that, notwithstanding any inconsistent term of this Agreement or any agreement between Customer and a Manufacturer, Symantec will be deemed a limited agent of Customer with respect to the services provided hereunder, and Customer represents that, prior to Customer's authorization of any Manufacturer to receive Certificates

hereunder, Customer will enter into a written Digital Certificate agreement with such Manufacturer stating such agency, providing Symantec with limitation of liability, disclaimer, and indemnity protection no less favorable than the terms hereof, and stipulating that the Manufacturer shall not be deemed a third party beneficiary of this Agreement. Customer shall be solely responsible for imposition and/or collection of any fees payable by Manufacturers in relation to the receipt of Certificates issued hereunder.

(d) Account Authorization. Customer shall provide Symantec advance written authorization of any Manufacturer authorized to receive Certificates issued hereunder, including such Manufacturer's contact information, identification of the individual(s) designated to be Service Administrator(s) for such Manufacturer (including enrollment information therefore), and the number of Certificates, sites, and/or Administrator Kits for which each Manufacturer has been authorized.

(e) Other Obligations. Customer shall ensure, and require its Manufacturer(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 such material or information. 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 Manufacturers.

(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, substantially in accordance with Symantec's standard PKI practices and policies, one CDCS Customer root CA Certificate and one CDCS CA Certificate issued under such CDCS root Certificate, which Certificates will be used solely for the purpose of providing the Service to Customer hereunder (or to other Symantec customers only upon Customer's express written consent). Additional CDCS CAs may be purchased separately.

(c) Provision of Service. Upon a Service Administrator's submission through the Service Console 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 Agreement (1) will have a validity period of twenty (20) years from the date the Certificate was issued, (2) must be requested in batch sizes not to exceed twenty-thousand (20,000) Certificates (larger batch requests and requests for Certificates with larger than 1024 bit key length may be rejected at Symantec's sole discretion), and (3) may not be integrated with or installed in any device which 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 Manufacturers 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).

(d) Account Activation. Subject to advance purchase through a Services Order, Symantec shall use commercially reasonably efforts to ship Administrator Kits for domestic sites within ten (10) days after receipt of Customer's authorization for the applicable Manufacturer, and within a commercially reasonable period for international sites to accommodate any special procedural or administrative requirements. Following Administrator Kit delivery, Symantec will use commercially reasonably efforts to activate domestic accounts within ten (10) business days and international accounts within a commercially reasonable period upon the following requirements being satisfied: (i) completion of the necessary enrollment process; (ii) authentication of the Manufacturer 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); and (iii) installing of the USB token, and download of the Service

Administrator Certificate into the USB token and the decryption utility.

(e) 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.