Symantec™ Certificate Lifecycle Platform Service Description

Introduction

Symantec™ Certificate Lifecycle Platform (CLP) provides a scalable Certification Authority service platform, and is designed for large in-premise configurations where a hosted and managed Public Key Infrastructure (PKI) solution is not appropriate due to regulatory, or other, factors. The product enables governments, and other large institutions, that cannot outsource any aspect of their PKI operations to have complete end-to-end control over their PKI infrastructure. Symantec™ CLP is capable of supporting millions of end user digital certificates on a global scale.

A PKI platform enables this level of security by making it possible for individuals with no prior contact to be authenticated with each other, maintain confidentiality, and establish the integrity of a message. PKI platforms accomplish this by employing a Certification Authority, which issues, renews, revokes, and manages digital certificates to deliver:

- Strong authentication (also known as "two-factor" authentication)
- Encryption
- Secure digital signing

Symantec Certificate Lifecycle Platform Architecture

The CLP architecture, based on Symantec™ Processing Center, is a set of hardware, software, and processes protected in a secure data facility. This facility functions as a primary Certification Authority (CA) to provide the full range of CA services to the enterprise and its end-users. Each enterprise is responsible for providing the secure facility, trusted employees, hardware and underlying system software that make up the physical components. Symantec provides the specifications, software, and secure processes that make up the non-physical components.

The front-end network hosts a combination of web servers to support incoming requests from both end users and remote enterprise administrators. The back-end network includes an application server(s) that oversees the processing of requests among the different back-end servers. These include:

- Database servers
- Signing servers (responsible for creating the signed certificates)
- Authentication servers (responsible for validating the enrollment data prior to approving certificate request)

Customer management and billing systems are typically configured in the back-end alongside the authentication servers.

The CLP enables enterprises to provide the following security services:

- Issuance of digital certificates to internal and external users
- Secure access to intranet and extranet applications
- Certificate lifecycle management
- Centralized key management solution

Features and Functionality

Standard CLP features enabled as part of the basic CLP installation include:

Managing Certification Authorities (CA) and their Keys

The CLP ships with the CA Key Management Tool and Administrator Management Tool that together provide functionality for configuring and managing CA keys in a secure and non-repudiable manner. The CA Key Management Tool allows for:

- Generation of CA key pairs
- Activation and deactivation CA certificates
- Maintenance of Certificate Revocation Lists (CRLs)

Hosting Administrator Services

The CLP includes RA administrator services to allow administrators to authenticate, approve or reject certificate requests from prospective subscribers, revoke certificates, and generate reports on certificate activity.

Hosting Subscriber Services

The CLP enables enterprises' end-users to access certificate lifecycle pages. The certificate lifecycle pages are Web pages that enable end-users to enroll for, retrieve, verify, suspend, and revoke their certificates. In addition, end-users can use a page to search for other end-users' certificates.

Logging and Maintaining Certificate Information

The CLP includes an Oracle database that, along with maintaining end-user/end-entity certificates, also tracks and saves information regarding administrative activities performed against a certificate. This data serves as an audit trail.

Business System API

The CLP can be integrated with enterprises' business system applications to allow automated billing, validation, and issuing functions.

Monitoring Tools

The CLP includes a set of software tools to monitor and manage critical system processes and applications. These monitoring tools can generate e-mail, alphanumeric pager messages, and console notifications.

Certificate Directory Search

The CLP enables enterprises' end-users to search the certificate database to look up certificate information for other end-users of the enterprise. Sharing certificate information increases the degree of interoperability between end-users.

Additional Modules

These features require additional equipment and/or additional purchases from Symantec. They include:

Key Management Service

This service provides the enterprise with a complete, centralized key management solution. It allows an enterprise administrator to control the backup and recovery of user private keys, with minimal risks and minimal security costs. This solution has three main functions: 1) generation and distribution of end user keys and certificates; 2) backup of private encryption keys; and 3) the recovery of those key and certificates.

Online Certificate Status Protocol (OCSP) Service

The OCSP Service allows an enterprises end-user to determine a certificates status (such as valid, revoked, or suspended) in real time, using the Online Certificate Status Protocol (OCSP) standards. OCSP may be an alternate to CRLs and may also be used to obtain additional status information.

General Considerations

Symantec also provides comprehensive customer support services, professional services, consulting assistance with CPS and CP policies, and a set of required training classes to enable the enterprise to operate and maintain the Symantec Certificate Lifecycle Platform effectively.

SYMANTEC CERTIFICATE LIFECYCLE PLATFORM ADDITIONAL TERMS AND CONDITIONS

1. DEFINITIONS

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

"Software" as used herein and defined in the Master Services Agreement means the CLP software licensed to Customer hereunder.

"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.

2. CUSTOMER'S OBLIGATIONS

(a) Customer Obligations. Customer is solely responsible for acquiring and maintaining requisite hardware on its premises (including any specialized devices such as third-party hardware security modules which are required by Symantec during installation) and maintaining the security of its network and computer systems. **IMPORTANT NOTE: WHILE THE SOFTWARE MAY BE CAPABLE OF ISSUING ELLIPTIC CURVE CRYPTOGRAPHY (ECC)-BASED CERTIFICATES, CUSTOMERS WHO CHOOSE TO DO SO MUST ENSURE THAT ITS HAS OBTAINED ALL THE REQUIRED INTELLECTUAL PROPERTY LICENSES TO THE ECC TECHNOLOGY APPLICABLE TO CUSTOMER'S USE CASE AND/OR JURISDICTION. SYMANTEC'S PROVISION OF THE CLP SOFTWARE DOES NOT INCLUDE SUCH RIGHTS.**

(b) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer hereby represents and warrants to Symantec that: (i) Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of the Software; (ii) with respect to any transfer of data from Customer to Symantec in connection with the Services contemplated herein, if any, Customer has obtained all necessary consents, rights in, licenses to, and authority over all such data necessary for Customer to permit Symantec to receive and process such data as contemplated herein including, but not limited to, Symantec's transfer of such data to United States and in other jurisdictions where Symantec maintains a presence; and (iii) Customer will use the Software exclusively for authorized and legal purposes consistent with this Agreement.

(c) 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) Installation. In order to optimize performance, Symantec shall provide Software installation services, including major and minor upgrades, at Symantec's then-current rates pursuant to a SOW or as set forth in the applicable order document. If additional work is required due to unusual or particularly-complex Customer systems or requirements, Customer may purchase additional consulting hours from Symantec. Symantec shall not be responsible for providing technical support to Customers who attempt to install or upgrade the Software on their own. However, such support may be purchased from Symantec's consulting services organization on an hourly basis, as needed.

(b) Services. Following completion of the requisite installation, all authentications, CA key pair generations, activation and deactivation of CA certificates and maintenance of CRLs shall be performed locally through the CLP.

(c) Acknowledgement of Delivery. The parties' execution of the order document applicable to this Service Description is appended shall confirm Symantec's delivery to Customer of the Software and related documentation, and Customer's acknowledgement of receipt thereof.

(d) Limited Warranty. Symantec warrants that the Software will operate in material conformance to Symantec's published specifications during the first ninety (90) days following Customer's initial receipt of the Software ("Warranty Period"). Symantec does

not warrant, however, that the Software or any portion thereof is error-free. If Customer discovers a non-conformity in the Software during the Warranty Period, Customer shall submit to Symantec a written report describing the non-conformity in sufficient detail to permit Symantec to reproduce such non-conformity. Upon confirmation by Symantec that the reported non-conformity has been reproduced and confirmed to be such by Symantec, Symantec will use reasonable efforts to, at its option, (i) correct the non-conformity; (ii) provide a work around or software patch (collectively "Fixes"); or (iii) replace the Software. If Symantec determines that none of these alternatives are reasonably available, upon Customer's request Symantec shall refund any license fees paid for the affected Software and accept its return. All Fixes provided by Symantec shall constitute Software as defined hereunder, as applicable, and shall be governed by the terms hereof. This warranty shall not apply to any non-conformity caused by any unauthorized modification to the Software or by Customer's failure to incorporate any Fixes provided by Symantec. This warranty applies only to the initial delivery of the Software. Fixes are provided with a limited warranty of thirty (30) days from receipt of such Fix or for the remainder of the initial Warranty Period, whichever is greater. The foregoing express warranties are in lieu of all liabilities or obligations on the part of Symantec. CUSTOMER'S SOLE REMEDY FOR BREACH OF WARRANTY SHALL BE A CORRECTION, FIX OR REFUND AS SET FORTH IN THIS SECTION.

4. EFFECT OF TERMINATION OF SERVICES

In the event of a termination of the Services contemplated herein for any reason: (i) Customer will immediately cease use of the Services and Software, (ii) the rights to use the Services and any related third-party software or other components will immediately terminate, (iii) Customer will permanently delete any Software related to the provision of the Services from any storage media upon which such Software is stored, and (iv) neither party shall be relieved of obligations or liabilities which accrued prior to the date of termination

5. AUDIT RIGHTS

Not more than twice a year, Symantec may audit and inspect, at its own expense, Customer's utilization of the Services contemplated in this Service Description in order to ensure compliance with the terms herein, the order document and the Agreement. Any such audit will be conducted during Customer's normal 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 underpaid fees to Symantec, such underpaid fees shall be immediately due and payable by Customer.