SymantecTrust Network (STN) Supplemental Certificate Policy and Certification Practice Statement for the Mortgage Industry PKI Service

Version 1.3

Published: 15 September 2011

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 650.527.8000
http//:www.symantec.com

Symantec Trust Network Supplemental Certificate Policy and Certification Practice Statement for the Mortgage Industry PKI Service

Important – Acquisition Notice

On August 9, 2010, Symantec Corporation completed the acquisition of VeriSign Inc's Authentication division. As a result Symantec is now the registered owner of this Certificate Practices Statement document and the PKI Services described within this document.

However a hybrid of references to both "VeriSign" and "Symantec" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

Acknowledgement

Symantec acknowledges the assistance of many reviewers of the document specializing in diverse areas of business, law, policy, and technology.

TABLE OF CONTENTS

1. Introduction

Please refer to the Acquisition Notice (page ii) for an explanation of the naming and ownership information referenced throughout this document.

The Symantec Mortgage Industry PKI Service no longer issues certificates to Subscribers. However this CPS is available to Relying Parties for questions regarding assurance of signatures on legacy documents signed by certificates issued by this CA.

This document, the Symantec Trust Network Supplemental Certificate Policy and Certification Practice Statement for the Symantec Mortgage Industry PKI Service referred to in this document as the "Mortgage Industry CP/CPS" and the singular acronym "CP/CPS"), [1] is a supplement to the Symantec Trust Network Certificate Policies ("CP") and Certification Practices Statement ("CPS"). The purpose of this CP/CPS is to document Symantec's policies and practices for the Symantec Mortgage Industry PKI Service, a service designed to meet the requirements of the mortgage industry as defined in the Mortgage Bankers Association - Secure Identity Services Accreditation Corporation's (MBA/SISAC) Certificate Policy Requirements Document, Version 1.3 draft dated June 18, 2003 ("CPRD"). The CPRD is intended to facilitate interoperability and the use of digital certificates ("Certificates") within the mortgage industry.

Please Note: The capitalized terms in this CP/CPS are defined terms with specific meanings. Please see the Acronyms and Definitions section for a list of definitions.

Symantec Corporation ("Symantec") is the leading provider of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals. The company's domain name, digital certificate, and payment services provide the critical web identity, authentication, and transaction infrastructure that online businesses require to conduct secure e-commerce and communications. The Symantec Trust Network ("STN") is a global public key infrastructure ("PKI") established to support the use of digital certificates for both wired and wireless applications. Symantec offers STN services together with a global network of affiliates ("Affiliates") throughout the world.

The CP is the principal statement of policy governing the STN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services. These requirements, called the "STN Standards," protect the security and integrity of the STN, apply to all STN Participants, and thereby provide assurances of uniform trust throughout the STN. More information concerning the STN and STN Standards is available in the CP.

Symantec and each Affiliate have authority over a portion of the STN. The portion of the STN controlled by Symantec or an Affiliate is called its "Sub-domain" of the STN. An Affiliate's Sub-domain consists of the portion of the STN under its control. An Affiliate's Sub-domain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

[1] Internal cross references to CP/CPS sections (*i.e.*, in the form of "CP/CPS §") are references to sections of this document.

Symantec and each of the Affiliates have a CPS that governs its Sub-domain within the STN. While the CP sets forth requirements that STN Participants must meet, the CPS describes how Symantec meets these requirements within Symantec's Sub-domain of the STN, which is primarily located in the United States. More specifically, the CPS describes the practices that Symantec employs for:

- securely managing the core infrastructure that supports the STN, and
- issuing, managing, revoking, and renewing STN Certificates

within Symantec's Sub-domain of the STN, in accordance with the requirements of the CP and its STN Standards.

This CP/CPS serves as a supplement to the CP and CPS and specifies Symantec's policies and practice that are specific to the Symantec Mortgage Industry PKI Service.

1.1 Overview

The Symantec Mortgage Industry PKI Service is based on Symantec's Managed PKI and retail certificate services, customized to meet the MBA/SISAC requirements.

This CP/CPS is specifically applicable to Symantec's Public CAs and the CAs of Managed PKI[2] Customers, which issue Certificates within the STN as part of Symantec's Mortgage Industry PKI Service. More generally, this CP/CPS also governs the use of STN services within Symantec's Sub-domain of the STN by all individuals and entities within Symantec's Sub-domain (collectively, Symantec Sub-domain Participants"). Private CAs and hierarchies managed by Symantec are outside the scope of this CP/CPS. The CAs managed by Affiliates are also outside the scope of this CP/CPS.

The STN includes three classes of Certificates, Classes 1-3, and the CP describes how these three Classes correspond to three classes of applications with common security requirements. The CP is a single document that defines three certificate policies, one for each of the Classes, and sets STN Standards for each Class.

The Symantec Mortgage Industry PKI Service has been designed to meet the requirements of the MBA/SISAC User Individual Basic and Medium, and User Organizational Medium assurance levels. Based on market needs, this service may be expanded to support the MBA/SISAC High assurance level in the future.

As part of the Symantec Mortgage Industry PKI Service, Symantec offers SISAC User Individual Basic and Medium Certificates (which are equivalent to STN Class 2 and 3 Certificates, respectively), and User Organizational Medium (which is equivalent to STN Class 3 Certificates). This CP/CPS describes how Symantec meets the CPRD requirements for SISAC User Individual Basic and Medium, and User Organizational Medium Certificates.

[2] The Managed PKI Service was formerly known as OnSite®. All references to OnSite and Client OnSite in this CPS have been changed to Managed PKI. Customers may still see references to OnSite in some VeriSign documentation and website URLs. The OnSite® Service itself has not changed.

(a) Role of Other Practices Documents

The CP describes at a general level the overall business, legal, and technical infrastructure of the STN. The CP is published in electronic form within the Symantec Repository at *www.symauth.com/repository/index.html*.

The CPS then applies STN Standards from the CP to Symantec Sub-domain Participants, and explains specific practices of Symantec in response to the CP. The CPS is published in electronic form within the Symantec Repository at *www.symauth.com/repository/index.html.*

This CP/CPS is intended to document Symantec's policies and practices for meeting the requirements of the CPRD. Examples include the Symantec Security Policy, the Security and Audit Requirements (SAR) Guide, the Enterprise Security Guide, and the Key Ceremony Reference Guide. These documents are above the Certification Practice Statements and Ancillary agreements used by Symantec or an Affiliate within the STN documentation architecture.

In addition, Symantec has established ancillary agreements that bind Customers, Subscribers, and Relying Parties of Symantec. Among other things, the agreements flow down STN Standards to these STN Participants and, in some cases, state specific practices for how they must meet STN Standards. Subscriber Agreements and Relying Party Agreements are published in the Symantec Repository. Managed PKI Agreements are confidential and are not published.

(b) Knowledge Assumed by This CP/CPS

This CP/CPS assumes that the reader is generally familiar with Digital Signatures, PKIs, Symantec's STN, and the CPRD. In addition, the CP/CPS assumes that the reader is familiar with the CP and CPS. If not, Symantec advises that the reader review the CP/CPS and the CPRD and obtain training in the use of public key cryptography and public key infrastructure as implemented in the STN. The CP/CPS contains references to such information and a brief summary of the roles of the STN participants. See CP § 1.1(b).

(c) Compliance with Applicable Standards

The practices specified in this CP/CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

The structure of this CP/CPS generally corresponds to the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. The RFC 2527 framework has become a standard in the PKI industry. This CP/CPS conforms to the RFC 2527 framework in order to make policy mapping and comparisons, assessment, and interoperation easier for persons using or considering using Symantec services.

Symantec has conformed the CP/CPS to the RFC 2527 structure where possible. While Symantec intends to continue the policy of adhering to RFC 2527 in the future, Symantec reserves the right to vary from the RFC 2527 structure as needed, for example to enhance the quality of the CP/CPS or its suitability to Symantec Sub-domain Participants. Moreover, the CP/CPS structure may not correspond to future versions of RFC 2527.

(d) Policy Overview

This CP/CPS defines three policies, *SISAC User Individual Basic* and *Medium* and *User Organizational Medium*, that are supplemental to the STN polices described in the CP.

The SISAC User Individual Basic policy corresponds to the *User Individual Basic Assurance* level defined in the CPRD. The *Basic Assurance* level is relevant to environments where the risks and consequences of data compromise are not considered by the Certificate Holder/Subscriber to be of major significance. This may include access to private information where the likelihood of malicious access is not high. SISAC *User Individual Basic assurance* Certificates defined by this CP/CPS are equivalent to STN *Class 2 individual Certificates* as defined by the CP.

The SISAC *User Individual Medium* policy corresponds to the *User Individual Medium Assurance* level defined in the CPRD. The *Medium Assurance* level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. SISAC *User Individual Medium assurance* Certificates defined by this CP/CPS are equivalent to STN *Class 3 individual Certificates* as defined by the CP.

The SISAC *User Organizational Medium* policy corresponds to the *User Organizational Medium Assurance* level defined in the CPRD. The *Medium Assurance* level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. SISAC *User Organizational Medium assurance* Certificates defined by this CP/CPS are equivalent to *Class 3 Organizational Certificates* as defined by the STN CP.

One of the functions of the CP is to describe the three Certificate Classes in detail.[3] Nonetheless, this section summarizes the Certificate Classes offered by Symantec as part of the Symantec Mortgage Industry PKI Service.

Class 2 Certificates offer a medium level of assurances in comparison with the other two Classes. Again, they are individual Certificates. In addition to the Class 1 validation procedures, Class 2 validation procedures add procedures based on a comparison of information submitted by the Certificate applicant against information in business records or databases or the database of a Symantec-approved identity proofing service. They can be used for digital signatures, encryption, and access control, including as proof of identity in medium-value transactions.

[3] *See* CP § 1.1.1.

Class 3 Certificates provide the highest level of assurances within Symantec's Subdomain. *Class 3 Certificates* are issued to individuals, organizations, and Administrators for CAs and RAs. *Class 3 individual Certificates* may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. *Class 3 individual Certificates* provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a person that confirms the identity of the Subscriber using, at a minimum, a well-recognized form of government-issued identification and one other identification credential. *Class 3 organizational Certificates* provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so.

Table 1 below summarizes the Certificate Classes offered by Symantec in compliance with the CP. It sets forth the properties of each Certificate class, based on whether they are issued to individuals or organizations, and whether they are offered on a Retail or Managed PKI basis or issued to Administrators.

The specifications for Classes of Certificates in the CP, as summarized in this CP/CPS, set forth the minimum level of assurances provided for each Class. Nonetheless, by contract or within specific environments (such as an intra-company environment), Symantec Subdomain Participants are permitted to use validation procedures stronger than the ones set forth within the CP, or use Certificates for higher security applications than the ones described in CP/CPS §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CP/CPS §§ 2.2.1.2, 2.2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

Class	***Issued to***	***Services Under Which Certificates are Available***[4]	***Confirmation of Certificate Applicants' Identity (CP/CPS §§ 3.1.8.1, 3.1.9)***	***Applications implemented or contemplated by Users (CP/CPS § 1.3.4.1)***
SISAC User Individual Basic (Class 2)	Individuals	Retail	Name and e-mail address search to ensure that the distinguished name is unique and unambiguous within the CA's Sub-domain, plus automated or Administrator-initiated enrollment information check with one or more third-party databases or comparable sources.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a medium level of assurances in comparison with the other Classes, such as some individual and intra- and inter-company e-mail, on-line subscriptions, account applications, and password
		Managed PKI	Name and e-mail address search as with SISAC User Individual Basic Retail plus	

[4] Retail Certificates are Certificates issued by VeriSign, acting as CA, to individuals or organizations purchasing certificates individually via the VeriSign web site. Managed PKI Certificates are based on a Certificate Application approved by a Managed PKI Customer that enters into a Managed PKI Agreement with VeriSign for the issuance of a certain quantity of Certificates (*see* CP § 1.1.2.1.1). Administrator Certificates are issued to CA or RA Administrators to allow them to perform administrative functions on behalf of the CA or RA.

Class	*Issued to*	*Services Under Which Certificates are Available*[4]	*Confirmation of Certificate Applicants' Identity (CP/CPS §§ 3.1.8.1, 3.1.9)*	*Applications implemented or contemplated by Users (CP/CPS § 1.3.4.1)*
			checking internal documentation or databases to confirm the Certificate Applicant's affiliation with the Managed PKI Customer as an Affiliated Individual plus checking internal documentation or databases to confirm identity of the Certificate Applicant (*e.g.*, human resources documentation).	replacement, including as proof of identity for medium-value transactions.
SISAC User Individual Medium (Class 3)	Individuals	Retail	Same as SISAC User Individual Basic Retail, plus personal presence and check of two or more ID credentials using Notary Public or equivalent.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurances in comparison with the other Classes, such as some online banking, corporate database access, and exchanging confidential information, including as proof of identity for high-value transactions.
		Managed PKI	Same as SISAC User Individual Basic Managed PKI, plus personal presence and check of two or more ID credentials using a Notary Public or equivalent.	
		Administrators	Specialized confirmation procedures depending upon the type of Administrator. The identity of the Administrator and the organization utilizing the Administrator are confirmed. *See also* CP/CPS § 5.2.3.	Administrator functions.
SISAC User Organizational Medium (Class 3)	Organizations	Retail	Check of third-party database or other documentation showing proof of right to use the organizational name. Validation check by telephone (or comparable procedure) to confirm information in, and authorization of, the Certificate Application.	Server and application authentication, confidentiality encryption, and (when communicating with other servers) client authentication (some examples include application servers that sign and encrypt XML transactions)

Table 1 - Certificate Properties Affecting Trust

1.1.1 Symantec Mortgage Industry PKI Service

The STN offers a series of services to assist in the deployment, management, and uses of Certificates, as described fully in CP § 1.1.2. The Symantec Mortgage Industry PKI Service is

based specifically on Symantec's Managed PKI and retail certificate services, customized to meet the MBA/SISAC requirements. All of such services are subject to the specific agreements with Symantec.

1.1.1.1 Symantec Managed PKI

As a "Processing Center," Symantec has established a secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates. Symantec acts as a CA in the STN and performs all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. It also provides CA key management and Certificate lifecycle services on behalf of its Managed PKI Customers.

Symantec Managed PKI is a fully integrated managed PKI service that allows enterprise Customers of Symantec to provide Certificates to individuals, such as employees, partners, suppliers, and customers. Within Symantec's Sub-domain, the security recommendations for Managed PKI are set forth in the Enterprise Security Guide. Managed PKI is an outsourcing service.

Customers of Symantec obtaining Symantec Managed PKI ("Managed PKI Customers") provide client Certificates by becoming a Certification Authority within Symantec's Sub-domain of the STN. Managed PKI Customers perform the RA "front-end" functions of approving or denying Certificate Applications, and initiating the revocation or renewal of Certificates using Managed PKI functionality. RA functions are a subset of CA functions. At the same time, the Managed PKI Customer can leverage the secure PKI backbone of the Symantec Trust Network by outsourcing all "back-end" Certificate issuing, management, revocation, and renewal functions to Symantec.

Symantec's Managed PKI Customers are not permitted to approve the Certificate Applications of anyone other than one of their own Affiliated Individuals, except as noted below. Managed PKI Customers may not approve Certificate Applications for STN Certificates issued to the general public.

1.1.1.2 Symantec Retail Certificate Services

Symantec also provides SISAC User Individual Basic and SISAC Medium, and User Organizational Certificates as a retail service to individuals. For this service, Symantec performs the CA function as well as the RA function.

1.1.1.3 Managed PKI Service Options

1.1.1.3.1 Symantec Managed PKI Key Management Services

Managed PKI Customers may optionally purchase Managed PKI Key Management Services that permits Managed PKI Customers to generate key pairs on behalf of Subscribers whose Certificate Applications they approve. It also permits Managed PKI Customers to transmit to

Subscribers the private keys of such Subscribers in a secure fashion, store a retained backup copy of the Subscribers' private keys in a secure fashion, and recover private keys when needed. Managed PKI Key Management Services facilitates both a single key pair system and a dual key pair system. Single key pair systems generate keys that an end-user Subscriber uses for both digital signature and confidentiality functions. The Subscriber obtains one Certificate for both functions. Dual key pair systems, by contrast, generate a key pair that the end-user Subscriber uses for confidentiality. The Subscriber, however, generates his or her own key pair for digital signature functions. In a dual key pair system, the Subscriber receives two Certificates, one for each public key. The Managed PKI Key Management Services software operates in conjunction with a Symantec Key Recovery Service. Managed PKI Key Management Services is described in detail in CP § 1.1.2.3.2.

Managed PKI Key Management Service software stores the backup copy of private keys at the Managed PKI Customer's site in an encrypted form. Each Subscriber's private key is individually encrypted with its unique key encryption key. A key recovery block ("KRB") is generated from this encryption key using key recovery technology, then the encryption key is deleted. Both the Subscriber's encrypted private key and the KRB are stored in the Key Manager database on the Managed PKI Customer's systems.

The Managed PKI Key Management Service software operates in conjunction with a Symantec Key Recovery Service. Recovery of a private key requires Managed PKI Key Management Service, under the Managed PKI Customer's administrator's direction, to retrieve the KRB from the database and send it online to the Key Recovery Service operated out Symantec's secure data center. Only Symantec holds the private key that can unlock the KRB and recover the embedded encryption key. The recovery request to Symantec will include enterprise emergency recovery codes needed to authorize the unlocking of the KRB. If a valid KRB is delivered, and the correct emergency recovery codes are supplied, the Key Recovery Service returns the encryption key to the Managed PKI Key Management Service software, allowing it to recover the corresponding user private key.

For purposes of the Symantec Mortgage Industry PKI Service, the Managed PKI Key Management Service shall not be used for backup of private signing keys.

1.2 Identification

This document is the Symantec Trust Network Supplemental Certificate Policy and Certification Practice Statement for the Mortgage Industry PKI Service. Under this CP/CPS, Symantec issues SISAC User Individual Basic and Medium, and User Organizational Medium Certificates. These Certificates contain object identifier values corresponding to the applicable assurance level.

Symantec, acting as a policy-defining authority, has assigned the supplemental certificate policy within this CP/CPS for each of SISAC User Individual Basic and Medium, and User Organizational an object identifier value extension set forth below.

The object identifier values used for SISAC User Basic and Medium are:

- SISAC User Individual Basic: Symantec/pki/policies/sisac/basic (2.16.840.1.113733.1.7.45.1).
- SISAC User Individual Medium: Symantec/pki/policies/sisac/medium (2.16.840.1.113733.1.7.45.2).
- SISAC User Organizational Medium: Symantec/pki/policies/sisac/medium (2.16.840.1.113733.1.7.45.2).

Certificate Policy Object Identifiers are used in accordance with CP/CPS § 7.1.6.

1.3 Community and Applicability

The community governed by the CPS is Symantec's Sub-domain within the Symantec Trust Network. The STN is a PKI that accommodates a worldwide, large, public, and widely distributed community of wired and wireless users with diverse needs for communications and information security. Symantec's Sub-domain of the STN is the portion of the STN governed by the CPS, and the CPS is the document that governs Symantec's Sub-domain of the STN.

This CP/CPS applies to users of the Symantec Mortgage Industry PKI Service which is a Sub-domain within the STN.

1.3.1 Certification Authorities

The term Certification Authority is an umbrella term that refers to all entities issuing Certificates within the STN. The term "CA" encompasses a subcategory of issuers called Primary Certification Authorities. PCAs act as roots of three domains, one for each class of Certificate. Each PCA is a Symantec entity. There are currently three generations of STN PCAs (G1, G2 and G3) for each class of Certificate. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs. CAs within Symantec's Sub-domain fall into two primary categories: (1) Symantec itself and (2) Managed PKI Customers. Symantec is a Processing Center that hosts the STN PCAs, its own CAs, and certain other CAs in its secure CA facilities.

Symantec performs all CA functions (including RA functions) for Symantec CAs. Managed PKI Customers become CAs within the STN. Managed PKI Customers outsource back-end functions to a Processing Center, while retaining RA functions for themselves.

A table at the following URL lists the Certification Authorities operated by Symantec within its Sub-domain of the STN: *www.symauth.com/repository/ca-ra.html*.

1.3.2 Registration Authorities

Within Symantec's Sub-domain of the STN, RAs are Managed PKI customers. Other types of RAs are permitted with Symantec's advance written consent and if these RAs meet the obligations placed on Managed PKI Customers, subject to any modifications necessary to account for any differences between Managed PKI technology and the technology used by these RAs and the terms of an appropriate agreement. RAs assist a CA by performing front-end

functions of confirming identity, approving or denying Certificate Applications, requesting revocation of Certificates, and approving or denying renewal requests.

A table at the following URL lists the entity or entities responsible for the Registration Authority function for each CA operated by Symantec within its Sub-domain of the STN: *http://www.symauth.com/repository/ca-ra.html*.

1.3.3 End Entities

Table 2 shows the types of Subscribers for each Class and type of Certificate offered within Symantec's Sub-domain of the STN as part of the Symantec Mortgage Industry PKI Service.

Class	*Issued to*	*Services Under Which Certificates are Available*	*Types of Subscribers*
SISAC User Individual Basic (Class 2)	Individuals	Retail	Any individual, including members of the general public.
		Managed PKI	Individuals who are, in relation to the Managed PKI Customer, an Affiliated Individual.
SISAC User Individual Medium (Class 3)	Individuals	Retail	Any individual, including members of the general public.
		Managed PKI	Individuals who are, in relation to the Managed PKI Customer, an Affiliated Individual.
		Administrators	Individuals serving in the role of Administrator (Trusted Persons who perform Certificate or certification service management functions on behalf of Symantec, Managed PKI Customers, or trusted fourth parties).
SISAC User Organizational Medium (Class 3)	Organizations	Retail	Organizations

Table 2 – Types of Subscribers within Symantec's Sub-domain of the STN

CAs are themselves Subscribers of Certificates, either as a PCA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "Subscribers" in this CPS, however, apply only to end-user Subscribers.

1.3.4 Applicability

This CP/CPS applies to all users of the Symantec Mortgage Industry PKI Service – specifically Symantec Sub-domain Participants, including Symantec, Customers, Subscribers, and Relying Parties. This CP/CPS applies to Symantec's Sub-domain of the STN and Symantec's core infrastructure supporting the STN.

This CP/CPS describes the practices governing the use of SISAC User Individual Basic and SISAC Medium, User Organizational Medium Certificates within Symantec's Sub-domain. SISAC User Individual Basic and Medium, and User Organizational Medium Certificates are generally appropriate for use with the applications set forth in CP § 1.3.4.1 and CP/CPS § 1.1 (Table 1). Nonetheless, by contract or within specific environments (such as an intra-company environment), STN Participants are permitted to use Certificates for higher security applications than the ones described in CP/CPS §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited

to such entities and subject to CP/CPS §§ 2.2.1.2, 2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.3.4.1 Suitable Applications

For suitable applications, *see* Section 1.1 Table 1. These listings, however, are not intended to be exhaustive]. Individual Certificates and some organizational Certificates permit Relying Parties to verify digital signatures. Symantec Sub-domain Participants acknowledge and agree, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to a STN Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Subject to applicable law, a digital signature or transaction entered into with reference to a STN Certificate shall be effective regardless of the geographic location where the STN Certificate is issued or the digital signature created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

1.3.4.2 Restricted Applications

In general, STN Certificates are general-purpose Certificates. STN Certificates may be used globally and to interoperate with diverse Relying Parties worldwide. Usage of STN Certificates is not generally restricted to a specific business environment, such as a pilot, financial services system, vertical market environment, or virtual marketplace. Nonetheless, such use is permitted and Customers using Certificates within their own environment may place further restrictions on Certificate use within these environments. Symantec and other Symantec Sub-domain Participants, however, are not responsible for monitoring or enforcing any such restrictions in these environments.

Nonetheless, certain STN Certificates are limited in function. For example, CA Certificates may not be used for any functions except CA functions. Moreover, client Certificates are intended for client applications and shall not be used as server or organizational Certificates. Further, Administrator Certificates shall only be used to perform Administrator functions.

Also, with respect to X.509 Version 3 STN Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a Certificate may be used within the STN. *See* CP § 6.1.9. In addition, end-user Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed through the use of the Basic Constraints extension. *See* CP § 7.1.2.4. The effectiveness of extension-based limitations, however, is subject to the operation of software manufactured or controlled by entities other than Symantec.

More generally, Certificates shall be used only to the extent use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

1.3.4.3 Prohibited Applications

STN Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of

nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.4 Contact Details

1.4.1 Specification Administration Organization

The organization administering this CP/CPS is the Symantec Practices Development group. Inquiries to Symantec's Practices Development group should be addressed as follows:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
Attn: Practices Development – CP/CPS
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
practices@symantec.com

1.4.2 Contact Person

Address inquiries about the CP/CPS to *practices@symantec.com* or to the following address:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
Attn: Practices Development – CPS
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)

1.4.3 Person Determining CPS Suitability for the Policy

The Symantec Practices Development group is responsible for determining the suitability of Symantec's practices to achieve Symantec's policy requirements.

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

CAs perform the specific obligations appearing throughout this CP/CPS

The provisions of the CPS specify obligations of each category of CAs: Symantec (in its role as Processing Center and manager of the core infrastructure that supports the STN) and Managed PKI Customers.

In addition, Symantec uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within Symantec's Sub-domain Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrollment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. The Subscriber Agreements and Relying Party Agreements used by Symantec must include the provisions required by CP/CPS §§ 2.2-2.4.

Managed PKI Customers are permitted to use Subscriber Agreements specific to them, although not required to do so. Managed PKI Customers using Subscriber Agreements must include the provisions required by CP §§ 2.2-2.4. If a Managed PKI Customer does not use its own Subscriber Agreement, the Subscriber Agreement of Symantec shall apply.

With Managed PKI, the Managed PKI Customer is the CA and outsources certain back end functions to Symantec. The Customer is also the RA unless the RA function is outsourced to Symantec.

2.1.2 RA Obligations

RAs assist Symantec by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests. The provisions of the CP/CPS specify obligations of RAs and are also outlined in contractual agreements.

2.1.3 Subscriber Obligations

Subscriber obligations in the CP apply to Subscribers within Symantec's Sub-domain, through the CPS and this CP/CPS, by way of Subscriber Agreements approved by Symantec. Certain Subscriber Agreements in force within Symantec's Sub-domain appear at: *http://www.symauth.com/repository/subscriber/index.html*

Within Symantec's Sub-domain, Subscriber Agreements require that Certificate Applicants provide complete and accurate information on their Certificate Applications and manifest assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

Subscriber Agreements apply the specific obligations appearing in the CP, CPS, and this CP/CPS to Subscribers in Symantec's Sub-domain. Subscriber Agreements require Subscribers to use their Certificates in accordance with CP/CPS § 1.3.4. They also require Subscribers to protect their private keys in accordance with CP/CPS §§ 6.1-6.2, 6.4. Under these Subscriber Agreements, if a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the activation data protecting such Private Key, or the information within the Certificate is incorrect or has changed, that the Subscriber must promptly:

- Notify the entity that approved the Subscriber's Certificate Application, either a CA or an RA, in accordance with CP/CPS § 4.4.1.1 and request revocation of the Certificate in accordance with CP/CPS §§ 3.4, 4.4.3.1, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements require Subscribers to cease use of their private keys at the end of their key usage periods under CP/CPS § 6.3.2.

Subscriber Agreements state that Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of the STN, except upon prior written approval from Symantec, and shall not otherwise intentionally compromise the security of the STN.

2.1.4 Relying Party Obligations

Relying Party obligations in the CP/CPS apply to Relying Parties within the Mortgage Industry PKI Service. Relying Party Agreements in force within Symantec's Sub-domain appear at: *http://www.symauth.com/repository/*

Relying Party Agreements within Symantec's Sub-domain state that before any act of reliance, Relying Parties must independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. They state that Symantec, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Party Agreements specifically state that Relying Parties must not use Certificates beyond the limitations in CP/CPS § 1.3.4.2 and for purposes prohibited in CP/CPS § 1.3.4.3.

Relying Party Agreements further state that Relying Parties must utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Under these Agreements, Relying Parties must not rely on a Certificate unless these verification procedures are successful.

Relying Party Agreements also require Relying Parties to check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CP/CPS §§ 4.4.10, 4.4.12. If any of the Certificates in the Certificate Chain have been revoked, according to Relying Party Agreements, the Relying Party must not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Finally, Relying Party Agreements state that assent to their terms is a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms under this section, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

Relying Party Agreements state that if all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Party Agreements state that Relying Parties must not monitor, interfere with, or reverse engineer the technical implementation of the STN, except upon prior written approval from Symantec, and shall not otherwise intentionally compromise the security of the STN.

2.1.5 Repository Obligations

Symantec is responsible for the repository functions for its own CAs and the CAs of its Managed PKI Customers. Symantec Customers issuing Certificates to end-user Subscribers publish Certificates they issue in the repository in accordance with CP/CPS § 2.6.

Upon revocation of an end-user Subscriber's Certificate, Symantec publishes notice of such revocation in its repository. Symantec issues CRLs for its own CAs and the CAs of Managed PKI Customers pursuant to CP/CPS §§ 2.6, 4.4.9, 4.4.11. In addition, for Managed PKI Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, Symantec provides OCSP services pursuant to CP/CPS §§ 2.6, 4.4.9, 4.4.11.

2.2 Liability

2.2.1 Certification Authority Liability

The warranties, disclaimers of warranty, and limitations of liability among Symantec and its Customers within Symantec's Sub-domain are set forth and governed by the agreements among them. This CP/CPS § 2.2.1 relates only to the warranties that certain CAs (Symantec and Managed PKI Customers) must make to end-user Subscribers receiving Certificates from them and to Relying Parties, the disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties.

Symantec uses Subscriber Agreements and Relying Party Agreements in accordance with CP/CPS § 2.1.1. Managed PKI Customers have the option of using a Subscriber Agreement. These Subscriber Agreements shall meet the requirements imposed by Symantec. Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to those Managed PKI Customers that use Subscriber Agreements. Symantec adheres to such requirements in its Subscriber Agreements. Symantec's practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to Symantec. Note that terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements, because Subscribers often act as Relying Parties as well.

2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties

Symantec's Subscriber Agreements include, and other Subscriber Agreements shall include, a warranty to Subscribers that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to this CPS in all material aspects.

Symantec's Relying Party Agreements contain a warranty to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate, except Non-verified Subscriber Information, is accurate,
- In the case of Certificates appearing in the Symantec Repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with CP/CPS § 4.3, and
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with this CPS when issuing the Certificate,
- The certificate is valid for use within a suitable application, as defined in Table 1 in Section 1.1, unless the certificate has been revoked.

2.2.1.2 Certification Authority Disclaimers of Warranties

To the extent permitted by applicable law, Symantec's Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, Symantec's possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the NetSure Protection Plan.

2.2.1.3 Certification Authority Limitations of Liability

To the extent permitted by applicable law, Symantec's Subscriber Agreements and Relying Party Agreements limit, and other Subscriber Agreements shall limit, Symantec's liability outside the context of the NetSure Protection Plan. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the following annual liability caps limiting Symantec's damages concerning a specific Certificate:

Class	*Annual Liability Caps*
SISAC User Individual Basic (Class 2)	Five Thousand U.S. Dollars ($ 5,000.00 US)
SISAC User Individual Medium (Class 3)	One Hundred Thousand U.S. Dollars ($ 100,000.00 US)
SISAC User Organizational Medium (Class 3)	One Hundred Thousand U.S. Dollars ($ 100,000.00 US)

Table 3 – Annual Liability Caps

Symantec will use commercially reasonable efforts to resolve claims made by subscribers and/or relying parties against Symantec within 120 days of Symantec's receipt of all requested documentation.

2.2.1.4 Force Majeure

To the extent permitted by applicable law, Symantec's Subscriber Agreements and Relying Party Agreements include, and other Subscriber Agreements shall include, a force majeure clause protecting Symantec.

2.2.2 Registration Authority Liability

The warranties, disclaimers of warranty, and limitations of liability between an RA and the CA it is assisting to issue Certificates are set forth and governed by the agreements between them.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber Warranties

Symantec's Subscriber Agreements require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- No unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Other Subscriber Agreements shall also contain these requirements.

Where a Subscriber's Certificate Application was approved by a Managed PKI Customer using the Managed PKI Key Manager offering, however, the Subscriber warrants only that no unauthorized person has ever had access to the copy of the Subscriber's private key on the Subscriber's hardware/software platform. These Subscribers make no warranty concerning the copies of their private keys in the possession of the Managed PKI Customers using Managed PKI Key Manager.

2.2.3.2 Private Key Compromise

The CP sets forth STN Standards for the protection of the private keys of Subscribers, which are included by virtue of CP/CPS § 6.2.7.1 in Subscriber Agreements. Subscriber Agreements state that Subscribers failing to meet these STN Standards are solely responsible for any loss or damage resulting from such failure.

2.2.4 Relying Party Liability

Subscriber Agreements and Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CP/CPS § 2.1.4.

2.3 Financial Responsibility

2.3.1 Insurance

Symantec's financial resources are set forth in disclosures appearing at: *http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-irhome*. Symantec maintains Professional Liability/Errors and Omissions Liability Insurance in the amount of not less than five million dollars ($5,000,000) including coverage for errors and omissions caused by Symantec's negligence in the performance of its duties under this Agreement.

Managed PKI Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. Managed PKI Customers shall also maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. This insurance requirement does not apply to governmental entities. Symantec maintains Professional Liability/Errors and Omissions Liability Insurance in the amount of not less than five million dollars ($5,000,000) including coverage for errors and omissions caused by Symantec's negligence in the performance of its duties under this Agreement.

2.3.2 Indemnification by Subscribers and Relying Parties

2.3.2.1 Indemnification by Subscribers

To the extent permitted by applicable law, Symantec's Subscriber Agreement require, and other Subscriber Agreements shall require, Subscribers to indemnify Symantec and any non-Symantec CAs or RAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,

- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.2.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Symantec's MBA Subscriber Agreements and MBA Relying Party Agreements require, and other Subscriber Agreements shall require, Relying Parties to indemnify Symantec, the Mortgage Bankers Association, and any non-Symantec CAs or RAs for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

2.3.3 Fiduciary Relationships

To the extent permitted by applicable law, Symantec's Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, any fiduciary relationship between Symantec or a non-Symantec CA or RA on one hand and a Subscriber or Relying Party on the other hand.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Subject to any limits appearing in applicable law, the laws of the State of California, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CP/CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in California, USA. This choice of law is made to ensure uniform procedures and interpretation for all SISAC PKI Participants, no matter where they are located.

This governing law provision applies only to this CP/CPS. The Symantec CP and CPS may have a different governing law provision See CPS §2.4.1. Agreements incorporating the CP/CPS by reference may have their own governing law provisions, provided that this CP/CPS § 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the CP/CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CP/CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, Symantec's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.3 Dispute Resolution Procedures

2.4.3.1 Disputes among Symantec and Customers

Disputes between Symantec and one of its Customers shall be resolved pursuant to provisions in the applicable agreement between parties.

2.4.3.2 Disputes between End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Symantec's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, a dispute resolution clause. The clause states that dispute resolution procedures require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing California, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

Symantec and Customers are entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

2.5.2 Certificate Access Fees

Symantec and Customers do not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

2.5.3 Revocation or Status Information Access Fees

Symantec does not charge a fee as a condition of making the CRLs required by CP/CPS § 4.4.9 available in a repository or otherwise available to Relying Parties[5]. Symantec does, however, charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. Symantec does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without Symantec's prior express written consent.

2.5.4 Fees for Other Services Such as Policy Information

Symantec does not charge a fee for access to the CP or this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, is subject to a license agreement with the entity holding the copyright to the document.

2.6 Publication and Repository

2.6.1 Publication of CA Information

Symantec is responsible for the repository function for:

- Symantec's Public Primary Certification Authorities (PCAs) and Symantec Infrastructure/Administrative CAs supporting the STN, and
- Symantec's CAs and Managed PKI Customers' CAs that issue Certificates within Symantec's Sub-domain of the STN.

Symantec publishes certain CA information in the repository at *http://www.symauth.com/repository/index.html* as described below.

- Symantec publishes this CP/CPS, the STN CP, the CPS, Subscriber Agreements, and Relying Party Agreements.
- Symantec publishes Certificates in accordance with Table 4 below.

Certificate Type	*Publication Requirements*
STN PCA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
STN Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Managed PKI Customer CA Certificates	Available through query of the LDAP directory server at *directory.verisign.com*.

[5] [5] VeriSign reserves the right to charge a fee in the future as a condition of making the CRLs required by CP/CPS §4.4.9 available in a repository or otherwise available to Relying Parties.

Certificate Type	*Publication Requirements*
Retail End-User Subscriber Certificates (Note: SISAC User Medium Organizational Certificates are not available in the repository)	Available to relying parties through a query function in the Symantec Repository at • *https://digitalid.verisign.com/services/client/index.html*. Also available through query of the LDAP directory server at *directory.verisign.com*.
End-User Subscriber Certificates issued through Managed PKI Customers	Made available through the query function listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.

Table 4 – Certificate Publication Requirements

Symantec publishes Certificate status information in accordance with CP/CPS § 4.4.11.

2.6.2 Frequency of Publication

Updates to this CP/CPS are published in accordance with § 8. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance according to § 2.6.1. Certificate status information is published in accordance with CP/CPS §§ 4.4.9 and 4.4.11.

2.6.3 Access Controls

Information published in the repository portion of the Symantec web site is publicly-accessible information. Read only access to such information is unrestricted. Symantec requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. Symantec has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.6.4 Repositories

See CP/CPS § 2.1.5.

2.7 Compliance Audit

An annual compliance audit is performed for Symantec's data center operations and key management operations supporting Symantec's public and Managed PKI CA services. In addition, an annual WebTrust for Certification Authorities examination is performed for the STN PCAs and Symantec's SISAC User Individual Medium and Basic, and User Organizational Medium CAs. Customer-specific CAs are not specifically audited as part of the audit of Symantec's operations unless required by the Customer. Symantec shall be entitled to require that Managed PKI Customers undergo a compliance audit under this CP/CPS § 2.7 and audit programs for these types of Customers.

In addition to compliance audits, Symantec shall be entitled to perform other reviews and investigations to ensure the trustworthiness of Symantec's Sub-domain of the STN, which include, but are not limited to:

- Symantec shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself or a Customer in the event Symantec has

reason to believe that the audited entity has failed to meet STN Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity's failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the STN.
- Symantec shall be entitled to perform "Supplemental Risk Management Reviews" on itself or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

Symantec shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with Symantec and the personnel performing the audit, review, or investigation.

2.7.1 Frequency of Entity Compliance Audit

Compliance audits are performed on an annual basis at the sole expense of the audited entity.

2.7.2 Identity and Qualifications of Auditor

Symantec's CA compliance audits are performed by a public accounting firm that:
- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and
- Is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

2.7.3 Auditor's Relationship to Audited Party

Compliance audits of Symantec's operations are performed by a public accounting firm that is independent of Symantec.

2.7.4 Topics Covered by Audit

The scope of Symantec's annual compliance audit includes CA environmental controls, CA key management, certificate life cycle management and CA business practices disclosure.

2.7.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of Symantec's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by Symantec management with input from the auditor. Symantec management is responsible for developing and implementing a corrective action plan.

If Symantec determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the STN, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. Symantec will notify SISAC of any deficiencies in the audit within forty-eight (48) hours.

For less serious exceptions or deficiencies, Symantec Management will evaluate the significance of such issues and determine the appropriate course of action.

2.7.6 Communications of Results

Results of the compliance audit of Symantec's operations may be released at the discretion of Symantec management.

2.8 Confidentiality and Privacy

Symantec has implemented a privacy policy, which is located at: *http://www.symantec.com/about/profile/privacypolicy/index.jsp* in compliance with CP § 2.8.

2.8.1 Types of Information to be Kept Confidential and Private

The following records of Subscribers are, subject to CP/CPS § 2.8.2, kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records (subject to CP/CPS § 2.8.2),
- Private keys held by Managed PKI Customers using Managed PKI Key Manager and information needed to recover such private keys,
- Transactional records (both full records and the audit trail of transactions),
- STN audit trail records created or retained by Symantec or a Customer,
- Symantec audit reports created by Symantec or their respective auditors (whether internal or public), except for WebTrust for Certification Authorities audit reports which may be published at the discretion of Symantec,
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of Symantec hardware and software and the administration of Certificate services and designated enrollment services.

2.8.2 Types of Information Not Considered Confidential or Private

Symantec Subdomain Participants acknowledge that Certificates, Certificate revocation and other status information, Symantec's repository, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under CP/CPS § 2.8.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See CP/CPS § 2.8.2.

2.8.4 Release to Law Enforcement Officials

Symantec Sub-domain Participants acknowledge that Symantec shall be entitled to disclose Confidential/Private Information if, in good faith, Symantec believes disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

2.8.5 Release as Part of Civil Discovery

Symantec Sub-domain Participants acknowledge that Symantec shall be entitled to disclose Confidential/Private Information if, in good faith, Symantec believes disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents. This section is subject to applicable privacy laws.

2.8.6 Disclosure Upon Owner's Request

Symantec's privacy policy contains provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to Symantec. This section is subject to applicable privacy laws.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

The allocation of Intellectual Property Rights among Symantec Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such Symantec Sub-domain Participants. The following subsections of CP/CPS § 2.9 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

2.9.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. Symantec and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. Symantec and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable Relying Party Agreement or any other applicable agreements.

2.9.2 Property Rights in the CP/CPS

Symantec Sub-domain Participants acknowledge that Symantec retains all Intellectual Property Rights in and to this CP/CPS.

2.9.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

2.9.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of Managed PKI Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, Symantec's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of Symantec. Symantec licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, without limiting the generality of the foregoing, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

While the STN is currently owned by Symantec Corporation, legacy certificates have been issued in the name of the former owner. Legacy certificates that indicates the Organization (O) as "VeriSign, Inc." and Organizational Unit (OU) as "VeriSign Trust Network" shall mean Symantec Corporation and the Symantec Trust Network, respectively.

CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. CA Distinguished Names consist of the components specified in Table 5 below.

Attribute	*Value*
Country (C) =	"US" or not used.
Organization (O) =	"Symantec Corporation"
Organizational Unit (OU) =	CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • CA Name • Symantec Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and • A copyright notice.
State or Province (S) =	Not used.
Locality (L) =	Not used.
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.

Table 5 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 6 below.

Attribute	*Value*
Country (C) =	"US".
Organization (O) =	Indicates the Subscriber's organizational name.
Organizational Unit (OU) =	End-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates). (This is non-verified subscriber information.) • Symantec Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Symantec" and "Member, Symantec Trust Network" in Certificates whose applications were authenticated by Symantec • Text to describe the type of Certificate.
State or Province (S) =	Indicates the Subscriber's Organization State or Province.
Locality (L) =	Indicates the Subscriber's Organization Locality.
Common Name (CN) =	.For User Individual certificate, this attribute includes the Subscriber's Individual Name. For User Organizational certificate, this attribute includes the verified Organization Name.
E-Mail Address (E) =	E-mail address for individual Certificates

Table 6 – Distinguished Name Attributes in End User Subscriber Certificates

The organization name value included in the Subject distinguished name of individual and organizational Certificates is the legal name of the organization. For individual Subscribers who are not associated with an organization, the organization name field will be excluded from the certificate.

The common name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

End-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate. For such Certificates, pseudonyms of end-user Subscribers (names other than a Subscriber's true personal or organizational name) are not permitted.

CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Uniqueness of Names

Symantec ensures that Subject Distinguished Names are unique within the domain of a specific CA through automated components of the Subscriber enrollment process.

3.1.5 Name Claim Dispute Resolution Procedure

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Symantec, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. Symantec is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.1.6 Recognition, Authentication, and Role of Trademarks

See CP/CPS § 3.1.5.

3.1.7 Method to Prove Possession of Private Key

Symantec verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically-equivalent demonstration, or another Symantec-approved method.

3.1.8 Authentication of Organization Identity

Symantec confirms the identity of the organization named in a Certificate Application in accordance with the procedures set forth in the subsections that follow.

3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers

3.1.8.1.1 Authentication for User Organizational Retail Certificates

Symantec confirms the identity of the organization included in the application for a Retail Certificate by:

- Verifying that the organization exists through the use of at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization and
- Confirming the employment of the listed Organizational contact with the Organization and further confirming with the listed Organizational contact by telephone, postal mail, or a comparable procedure certain information about the organization and, that the organization has authorized the Certificate Application.

3.1.8.1.2 Authentication for Managed PKI

With respect to Managed PKI Customers, the identity confirmation process begins with Symantec's confirmation of the identity of the Managed PKI Customer itself in accordance with CP/CPS § 3.1.8.2. Following such confirmation, the Managed PKI Customer is responsible for approving the issuance of Certificates to individuals within its own organization in accordance with CP/CPS §3.1.9.

3.1.8.2 Authentication of the Identity of CAs and RAs

For CA Certificate Applications, certificate requests are created, processed and approved by authorized Symantec personnel using a controlled process that requires the participation of multiple trusted Symantec employees.

Managed PKI Customers enter into an agreement with Symantec before becoming CAs or RAs. Symantec authenticates the identity of the prospective Managed PKI Customer before final approval of its status as CA or RA by performing the checks required for the confirmation of the identity of organizational end-user Subscribers specified in CP/CPS § 3.1.8.1, except that instead of a Certificate Application, the validation is of an application to become a Managed PKI Customer. In addition, Symantec confirms that the person identified as Managed PKI Administrator is authorized to act in that capacity. Optionally, Symantec may require the personal appearance of an authorized representative of the organization before authorized Symantec personnel.

3.1.9 Authentication of Individual Identity

For SISAC User Individual Basic and Medium, and User Organizational certificates, Symantec or a Managed PKI Customer confirms that:

- the Certificate Applicant is the person identified in the Certificate Application,
- the Organization named in the Certificate Application exists in accordance with CP/CPS §3.1.8.1.1,
- the Certificate Applicant is an employee of the Organization named in the Certificate Application in accordance with CP/CPS §3.1.8.1.1,
- the Certificate Applicant rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CP/CPS § 3.1.7, and
- the information to be included in the Certificate is accurate, except for Nonverified Subscriber Information.

In addition, Symantec performs the more detailed procedures described below for each Class of Certificate.

3.1.9.1 SISAC User Individual Basic Individual Certificates

Authentication of SISAC User Individual Basic Certificates takes place in one of two ways. For SISAC Basic Managed PKI Certificates, Managed PKI Customers use business records or databases of business information to approve or deny Certificate Applications in accordance with CP/CPS § 3.1.9.2.1. For SISAC User Individual Basic Retail Certificates, Symantec confirms

the identity of Certificate Applicants using information residing in the database of a Symantec-approved identity proofing service in accordance with CP/CPS § 3.1.9.2.2.

3.1.9.1.1 SISAC User Individual Basic Managed PKI Certificates

For SISAC User Individual Basic Managed PKI Certificates, the Managed PKI Customer approves Certificate Applications using manual or automated authentication procedures or passcodes as discussed below.

Managed PKI Customers confirm the identity of individuals by comparing enrollment information against their own business records or databases of business information. For example, they may check enrollment information against employee or independent contractor records in a human resources department database. The Managed PKI Customer may approve the Certificate Application manually using the Managed PKI Control Center if the enrollment information matches the records or database used for authentication. This process is known as "Manual Authentication."

Managed PKI's Automated Administration Software Module and other similar Symantec software give Managed PKI Customers the option of automatic approval and revocation of users directly from pre-existing administrative systems or databases, rather than requiring Manual Authentication for each Certificate Application. Managed PKI Customers using the Managed PKI Automated Administration Software Module authenticate the identity of potential Certificate Applications before placing their information in a database. When a Certificate Applicant submits a Certificate Application, then, the Automated Administration Software Module compares information in the Certificate Application with the database and, if the information matches, automatically approves the Certificate Application for immediate issuance by Symantec. This process is called "Automated Administration."

Symantec Managed PKI "Passcode" authentication ("Passcode Authentication") involves the automatic approval or rejection of Certificate Applications by comparing a Certificate Applicant's enrollment data with pre-configured authentication data that are provided by a Managed PKI Customer's Managed PKI Administrator. With Passcode Authentication, the Managed PKI Customer uses an offline process to distribute "passcodes" to prospective Certificate Applicants that have satisfied the appropriate level of authentication. The Certificate Applicant then provides this passcode when submitting a Certificate Application, along with other authentication information. The passcode and additional authentication information are compared to the passcode database previously configured by the Managed PKI Administrator, and if all the fields match, a Certificate is issued.

Managed PKI Customers not using Automated Administration or Passcode Authentication must use Manual Authentication.

3.1.9.1.2 SISAC User Individual Basic Retail Certificates

Symantec validates Certificate Applications for SISAC User Individual Basic Retail Certificates by determining if identifying information in the Certificate Application matches information residing in the database of a Symantec-approved identity proofing service, such as a major credit

bureau or other reliable source of information providing services. If the information in the Certificate Application matches the information in the database, Symantec may approve the Certificate Application.

3.1.9.2 SISAC User Individual Medium Individual Certificates

3.1.9.2.1 SISAC User Individual Medium Managed PKI Certificates

The authentication of SISAC User Individual Medium individual Managed PKI Certificate Applications is based on the personal (physical) presence of the Certificate Applicant before a Managed PKI Administrator, notary public, or other official with comparable authority within the Certificate Applicant's jurisdiction. The Managed PKI Administrator, notary or other official checks the identity of the Certificate Applicant against:

- a well-recognized form of government-issued picture identification (e.g., a passport or driver's license) and
- one other identification credential (e.g., a currently-valid major credit card, an employer identification card with employer name and street address, a social security card, or a utility bill with a matching name and address).

Upon completion of this identity check, the Managed PKI Administrator, notary or other official signs a declaration indicating that the check was performed in accordance with this CP/CPS.

The Certificate Applicant is also required to a sign a declaration of identity using a handwritten signature.

3.1.9.2.2 SISAC User Individual Medium Retail Certificates

The authentication of SISAC User Individual Medium individual Certificate Applications is based on the personal (physical) presence of the Certificate Applicant before an authorized Symantec representative notary public with comparable authority within the Certificate Applicant's jurisdiction. The Symantec representative, notary or other official checks the identity of the Certificate Applicant against:

- a well-recognized form of government-issued picture identification (e.g., a passport or driver's license) and
- one other identification credential (e.g., a currently-valid major credit card, an employer identification card with employer name and street address, a social security card, or a utility bill with a matching name and address).

Upon completion of this identity check, the Symantec representative, notary or other official signs a declaration indicating that the check was performed in accordance with this CP/CPS.

The Certificate Applicant is also required to a sign a declaration of identity using a handwritten signature.

3.1.9.2.3 SISAC Administrator Certificates

Administrator Certificates are used to control access to Symantec CA systems and for authorizing certain actions within the STN.

Symantec authenticates SISAC Administrator Certificate Applications for Managed PKI Customers as follows:

- Symantec authenticates the existence and identity of the entity employing or retaining the Administrator pursuant to CP/CPS § 3.1.8.2
- Symantec confirms the employment and authorization of the person named as Administrator in the Certificate Application to act as Administrator.

Symantec also approves Certificate Applications for its own Administrators. Administrators are "Trusted Persons" within their respective organization (see CP/CPS § 5.2.1). In this case, authentication of their Certificate Applications is based on confirmation of their identity in connection with their employment or retention as an independent contractor (see CP/CPS § 5.2.3), background checking procedures (see CP/CPS § 5.3.2), and authorization to act as Administrator. In addition, Symantec performs the steps specified in CP/CP § 3.1.9.2.2.

3.2 Routine Rekey and Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. Symantec generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey"). However, in certain cases (e.g., CA certificates), Symantec permits Subscribers to request a new certificate for an existing key pair (technically defined as "renewal"). Table 7 below describes Symantec's requirements for routine rekey (issuance of a new certificate for a new key pair that replaces an existing key pair) and renewal (issuance of a new certificate for an existing key pair).

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal," focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all end-user Subscriber Certificates, this distinction is not important as a new key pair is always generated as part of Symantec's end-user Subscriber Certificate replacement process. In addition, new CA Certificates may be issued for existing CA key pairs subject to the constraints specified in Table 7 below.

Certificate Type	*Routine Rekey and Renewal Requirements*
CA Certificates	Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicable maximum CA key pair lifetime specified in CP/CPS § 6.3.2. CAs may also be rekeyed in accordance with CP/CPS § 4.7. Accordingly, for CA Certificates both rekey and certificate renewal are supported.
RA Certificates	For these Certificates, rekey is required.

Certificate Type	*Routine Rekey and Renewal Requirements*
SISAC User Individual Basic and Medium end-user Subscriber Certificates	For these types of Certificates, Subscriber key pairs are browser generated as part of the online enrollment process. The Subscriber does not have the option to submit an existing key pair for "renewal." Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not.

Table 7 – Routine Rekey and Renewal Requirements

3.2.1 Routine Rekey and Renewal for End-User Subscriber Certificates

Subscriber Certificates, which have not been revoked, may be replaced (i.e., rekeyed or renewed) in accordance with the Table 8 below.

Timing	*Requirement*
Before Certificate expiration	For SISAC User Basic and Medium Certificates, Symantec or the Managed PKI Customer authenticates Subscribers seeking Certificate replacement in accordance with the requirements specified in CP/CPS § 3.1.8.1 and 3.1.9 for the authentication of an original Certificate Application, with the exception that SISAC User Medium certificates may be replaced up to a specified number of times without requiring in person presence.
After Certificate expiration	In this scenario, the requirements specified in CP/CPS § 3.1.8.1 and 3.1.9 for the authentication of an original Certificate Application are used for replacing an end-user Subscriber Certificate.

Table 8 – Routine Rekey and Renewal Requirements for End-User Subscriber Certificates

3.2.2 Routine Rekey and Renewal for CA Certificates

CAs may be rekeyed periodically in accordance with CP/CPS § 4.7.

CA Certificates may be renewed within the parameters specified in CP/CPS § 6.3.2. For example, if an initial PCA certificate was issued with a lifetime of 10 years, renewed certificates may be issued to extend the validity period of the CA's key pair for an additional 20 years, reaching the maximum permitted validity period of 30 years. CA Certificate Renewal is not permitted after Certificate Expiration.

For Symantec self-signed PCA Certificates, other STN Root CAs, and CA Certificates, renewal requests are created and approved by authorized Symantec personnel through a controlled process that requires the participation of multiple trusted individuals.

For non-Symantec CA Certificates which chain to the STN PCAs, Symantec performs appropriate procedures to verify that the Managed PKI Customer is in fact the Subscriber of the CA Certificate. Authentication procedures are the same as original enrollment pursuant to CP/CPS § 3.1.8.2.

3.3 Rekey After Revocation

Rekey after revocation is not be permitted if:

- revocation occurred because the Certificate was issued to a person other than the one named as the Subject of the Certificate,

- the Certificate was issued without the authorization of the person named as the Subject of such Certificate, or
- The entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.

Subject to the foregoing paragraph, the requirements specified in CP/CPS §§ 3.1.8.1, § 3.1.9 for the authentication of an original Certificate Application shall be used for replacing an end-user Subscriber Certificate that has been revoked.

3.4 Revocation Request

Prior to the revocation of a Certificate, Symantec verifies that the revocation has been requested by the Certificate's Subscriber or the entity that approved the Certificate Application. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber submit the Subscriber's Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

Symantec Administrators are entitled to request the revocation of end-user Subscriber Certificates within Symantec's Sub-domain. Symantec authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

Managed PKI Customers using the Automated Administration Software Module may submit bulk revocation requests to Symantec. Such requests are authenticated via a request digitally signed with the private key in the Managed PKI Customer's Automated Administration hardware token.

The requests of Managed PKI Customers to revoke a CA Certificate are authenticated by Symantec to ensure that the revocation has in fact been requested by the CA.

4. Operational Requirements

4.1 Certificate Application

4.1.1 Certificate Applications for End-User Subscriber Certificates

All end-user Certificate Applicants shall undergo an enrollment process consisting of:

- completing a Certificate Application and providing the required information
- generating a key pair in accordance with CP/CPS § 6.1,

- the Certificate Applicant delivering his or her public key, directly or through an Managed PKI Customer, to Symantec in accordance with CP/CPS § 6.1.3,
- demonstrating to Symantec pursuant to CP/CPS § 3.1.7 that the Certificate Applicant has possession of the private key corresponding to the public key delivered to Symantec, and
- Manifesting assent to the relevant Subscriber Agreement.

Certificate Applications are submitted either to Symantec or Managed PKI Customer for processing, with result being either approval or denial. The entity processing the Certificate Application and the entity issuing the Certificate pursuant to CP/CPS § 4.2 may be two different entities as shown in the following table.

Certificate Class/Category	*Entity Processing Certificate Applications*	*Entity Issuing Certificate*
CA Certificate	Symantec	Symantec
SISAC Administrator Certificate	Symantec	Symantec
SISAC User Basic individual Retail Certificate	Symantec	Symantec
SISAC User Basic individual Managed PKI Certificate	Managed PKI Customer	Symantec
SISAC User Medium individual Retail Certificate	Symantec	Symantec
SISAC User Medium individual Managed PKI Certificate	Managed PKI Customer	Symantec
SISAC User Medium Organizational retail Certificate	Symantec	Symantec

Table 9 – Entities Receiving Certificate Applications

4.1.2 Certificate Applications for CA and RA Certificates

4.1.2.1 CA Certificates

The PCAs issue certificates only to CAs subordinate to them, including Symantec and Managed PKI Customer CAs. For Symantec CAs certificate requests are created and approved by authorized Symantec personnel through a controlled process that requires the participation of multiple trusted individuals.

Managed PKI Customers, which are subscribers of CA Certificates, enter into a contract with Symantec. CA Certificate Applicants are required to provide their credentials as required by CP/CPS § 3.1.8.2 to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a Managed PKI Customer's CA key pair, the applicant shall cooperate with Symantec to determine the appropriate distinguished name and the content of the Certificates to be issued to the applicant. For these CAs, certificate requests are created and approved by authorized Symantec personnel through a controlled process that requires the participation of multiple trusted individuals.

4.1.2.2 RA Certificates

Symantec operates several administrative CAs, which issue certificates to RAs and RA systems including:

- Symantec personnel (Symantec RA Administrators) who process Certificate Applications on behalf of Symantec CAs,
- Managed PKI Customer personnel (Managed PKI Administrators) who process Certificate Applications on behalf of the Managed PKI Customer within their organization,
- Automated Administration servers, which process Certificate Applications for Managed PKI Customers where an Automated Administration authentication process has been established.

For all of these RAs, as subscribers to the relevant Administrative CA, the requirements for Administrator Certificates specified in CP/CPS § 4.1.1 apply.

4.2 Certificate Issuance

4.2.1 Issuance of End-User Subscriber Certificates

After a Certificate Applicant submits a Certificate Application, Symantec or a Managed PKI Administrator, (see CP/CPS § 4.1.1) attempts to confirm the information in the Certificate Application (other than Non-Verified Subscriber Information) pursuant to CP/CPS §§ 3.1.8.1, 3.1.9. Upon successful performance of all required authentication procedures pursuant to CP/CPS § 3.1, Symantec or a Managed PKI Administrator approves the Certificate Application. If authentication is unsuccessful, Symantec or a Managed PKI Administrator denies the Certificate Application.

A Certificate is created and issued following the approval of a Certificate Application or following receipt of an RA's request to issue the Certificate. Symantec creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application. When a Managed PKI Customer approves a Certificate Application and communicates the approval to Symantec, Symantec creates a Certificate and issues it to the Certificate Applicant. The procedures of this section are also used for the issuance of Certificates in connection with the submission of a request to replace (i.e., renew or rekey) a Certificate.

Symantec or the Managed PKI Administrator shall respond promptly to Certificate Applications and provide updates regarding application status upon request.

4.2.2 Issuance of CA and RA Certificates

Symantec authenticates the identity of entities wishing to become Customers in accordance with CP/CPS § 3.1.8.2 and, upon approval, issues the Certificates needed to perform their CA or RA functions. Before Symantec enters into a contract with a Customer applicant under CP/CPS § 4.1.2, the identity of the potential Customer is confirmed based on the credentials presented. The execution of such a contract indicates the complete and final approval of the application by Symantec. The decision to approve or reject a Customer application is solely at the discretion of Symantec. Following such approval, Symantec issues the Certificate to the Customer CA or RA in accordance with CP/CPS § 6.1.

4.3 Certificate Acceptance

Upon Certificate generation, Symantec notifies Subscribers that their Certificates are available and notifies them of the means for obtaining such Certificates. For Managed PKI Customers, Subscribers are notified through the Managed PKI Administrator.

Upon issuance, Certificates are made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate. For example, Symantec may send the Subscriber a PIN, which the Subscriber enters into an enrollment web page to obtain the Certificate. The Certificate may also be sent to the Subscriber in an e-mail message. Downloading a Certificate, or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

4.4.1.1 Circumstances for Revoking End-User Subscriber Certificates

An end-user Subscriber Certificate is revoked if:

- Symantec, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- Symantec or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- Symantec or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
- Symantec or a Customer has reason to believe that a material fact in the Certificate Application is false,
- Symantec or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed, or
- The Subscriber requests revocation of the Certificate in accordance with CP/CPS § 3.4.

Symantec may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

Symantec Subscriber Agreements require end-user Subscribers to immediately notify Symantec of a known or suspected compromise of its private key in accordance with the procedures in CP/CPS § 4.4.3.1.

4.4.1.2 Circumstances for Revoking CA or RA Certificates

Symantec will revoke CA or RA Certificates if:

- Symantec discovers or has reason to believe that there has been a compromise of the CA or RA private key,
- The agreement between the CA or RA with Symantec has been terminated,
- Symantec discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CP/CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate,
- Symantec determines that a material prerequisite to Certificate issuance was neither satisfied nor waived, or
- The CA or RA requests revocation of the Certificate.

Symantec requires that Managed PKI Customers notify Symantec when revocation is required in accordance with the procedures in CP/CPS § 4.4.3.1.

4.4.2 Who Can Request Revocation

4.4.2.1 Who Can Request Revocation of an End-User Subscriber Certificate

The following entities may request revocation of an end-user Subscriber Certificate:

- Symantec or the Customer that approved the Subscriber's Certificate Application may request the revocation of any end-user Subscriber or Administrator Certificates in accordance with CP/CPS § 4.4.1.1.
- Individual Subscribers may request revocation of their own individual Certificates.
- In the case of organizational Certificates, only a duly authorized representative of the organization is entitled to request the revocation of Certificates issued to the organization.
- A duly authorized representative of Symantec or a Managed PKI Customer whose Administrator received an Administrator Certificate is entitled to request the revocation of an Administrator's Certificate.

4.4.2.2 Who Can Request Revocation of a CA, RA, or Infrastructure Certificate

The following entities may request revocation of a CA, RA, or infrastructure Certificate:

- Only Symantec is entitled to request or initiate the revocation of the Certificates issued to its own CAs, RAs, or infrastructure components.
- Symantec may initiate the revocation of any Symantec CA, Managed PKI Customer, RA, or infrastructure Certificate in accordance with CP/CPS § 4.4.1.2.
- Managed PKI Customers are entitled, through their duly authorized representatives, to request the revocation of their own CA, RA, and infrastructure Certificates.

4.4.3 Procedure for Revocation Request

4.4.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to Symantec or the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. For Managed PKI customers, the Subscriber is required to communicate the request to the Managed PKI Administrator who will communicate the revocation request to Symantec for processing. Communication of such revocation request shall be in accordance with CP/CPS § 3.4.

Where a Managed PKI Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer instructs Symantec to revoke the Certificate.

4.4.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to Symantec. Symantec will then revoke the Certificate. Symantec may also initiate CA or RA Certificate revocation.

4.4.4 Revocation Request Grace Period

Revocation requests must be submitted as promptly as possible within a commercially reasonable period of time. A revocation request that is authenticated and approved will be processed as promptly as possible, generally within forty-eight (48) hours.

4.4.5 Circumstances for Suspension

Symantec does not offer suspension services for CA or end-user Subscriber Certificates.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency

Symantec publishes CRLs showing the revocation of Certificates as follows:

CA Type	*CRL Frequency*
CAs that issue SISAC User Individual Basic end-user Subscriber Certificates	Daily
CAs that issue SISAC User Individual Medium end-user Subscriber Certificates	Every 12 hours[6]
CAs that issue SISAC Medium User Organizational end-user Subscriber Certificates	At least weekly
CAs that only issue CA Certificates	Quarterly and also whenever a CA Certificate is revoked

Table 10 – CRL Issuance Frequency

Expired Certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration.

4.4.10 Certificate Revocation List Checking Requirements

Relying Parties must check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

- For PCAs, SISAC User Individual Basic CAs, and SISAC User Individual Medium CAs, CRLs are posted in the Symantec Repository at *http://crl.verisign.com*.
- For SISAC Medium User Organizational CAs, CRLs are posted in the Symantec Repository at *http://mba-server-crl.verisign.com*
- For Managed PKI Customer CAs, CRLs are posted in customer-specific repositories, the location of which is communicated to the Managed PKI customer.

A "CRL reference Table" is also posted in the Repository to enable Relying Parties to determine the location of the CRL for the relevant CA.

4.4.11 On-Line Revocation/Status Checking Availability

This section does not apply for SISAC Medium User Organizational Certificates and CAs.

In addition to publishing CRLs, Symantec provides Certificate status information through web-based query functions accessible through the Symantec Repository at *https://digitalid.verisign.com/services/client/index.html*.

Symantec also provides OCSP Certificate status information. Managed PKI Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Managed PKI Customer.

Symantec OCSP Responders are configured to:

- log all certificate status requests;
- digitally sign all status responses; and

[6] This requires VeriSign's Premium CRL service.

- log all status responses.

4.4.12 On-Line Revocation Checking Requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party must check Certificate status using one of the applicable methods specified in CP/CPS § 4.4.11.

Relying Parties who use OCSP for certificate status checking must validate a Certificate with such online revocation status services before relying on the Certificate and maintain a log of the validation request. Failure to follow this process negates the ability of the Relying Party to claim that it acted on a Certificate with Reasonable Reliance.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Regarding Key Compromise

If Symantec discovers that there has been a compromise of the private key of a Symantec CA, Symantec shall revoke the certificate and notify Relying Parties, by publishing the revocation in the applicable CRL per CP/CPS §§ 4.4.9. Publication of revocation will happen within 24 hours of completion of due diligence.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

Symantec manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by Symantec personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity

- CA facility visitor entry/exit
- Security incidents.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

Symantec RAs and Managed PKI Administrators log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's drivers license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

All electronic and non-electronic security audit logs are retained and made available during audits.

4.5.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, Symantec reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within Symantec CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are documented.

4.5.3 Retention Period for Audit Log

Audit logs are retained onsite at least two (2) months after processing and thereafter archived in accordance with CP/CPS § 4.6.2.

4.5.4 Protection of Audit Log

Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

4.5.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

4.5.6 Audit Collection System

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by Symantec personnel.

4.5.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

Symantec performs periodic vulnerability assessments of its production environment. The results of such assessments are used to enhance the security of the environment.

4.6 Records Archival

4.6.1 Types of Events Recorded

In addition to the audit logs specified in CP/CPS § 4.5, Symantec maintains records that include documentation of:

- Symantec's compliance with the CPS and other obligations under its agreements with their Subscribers, and
- actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and rekey or renewal of all Certificates issued from the Symantec Processing Center.

Symantec's records of Certificate life cycle events include:

- the identity of the Subscriber named in each Certificate,
- the identity of persons requesting Certificate revocation,
- other facts represented in the Certificate,
- time stamps, and
- certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a Compliance Audit under CP/CPS § 2.7.

Records may be maintained electronically or in hard copy, provided that such records are accurately and completely indexed, stored, preserved, and reproduced.

4.6.2 Retention Period for Archive

Records associated with a Certificate are retained for at least the time periods set forth below following the date the Certificate expires or is revoked:

- Ten (10) years for SISAC User Individual Basic Certificates, and
- Thirty (30) years for SISAC User Medium Certificates.

If necessary, Symantec may implement longer retention periods in order to comply with applicable laws.

4.6.3 Protection of Archive

Symantec protects its archived records compiled under CP/CPS § 4.6.1 so that only authorized Trusted Persons are permitted to access archived data. Electronically archived data is protected against unauthorized viewing, modification, deletion, or other tampering through the implementation of appropriate physical and logical access controls. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archived data can be accessed for the time period set forth in CP/CPS § 4.6.2.

4.6.4 Archive Backup Procedures

Symantec incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records compiled under CP/CPS § 4.6.1 are maintained in an off-site disaster recovery facility in accordance with CP/CPS § 4.8.

4.6.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. It should be noted that such time information is not cryptographic-based.

4.6.6 Procedures to Obtain and Verify Archive Information

See CP/CPS § 4.6.3.

4.7 Key Changeover

STN CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in CP/CPS § 6.3.2. STN CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with CP/CPS § 6.1.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). Symantec's CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than sixty (60) days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

- The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

4.8 Disaster Recovery and Key Compromise

Symantec has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise or disaster. In addition, Symantec has implemented disaster recovery procedures described in CP/CPS § 4.8.2 and Key Compromise response procedures described in CP/CPS § 4.8.3. Symantec's Compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore Symantec's operations within a commercially reasonable period of time.

4.8.1 Corruption of Computing Resources, Software, and/or Data

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Symantec Security and Symantec's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Symantec's key compromise or disaster recovery procedures will be enacted.

4.8.2 Disaster Recovery

Symantec has implemented a disaster recovery site more than 1000 miles from Symantec's principal secure facilities. Symantec has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. Symantec's disaster recovery site has implemented the physical security protections and operational controls required by the Security and Audit Requirements (SAR) Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from Symantec's primary facility, Symantec's disaster recovery process is initiated by the Symantec Emergency Response Team (SERT).

Symantec has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- publication of revocation information, and
- provision of key recovery information for Managed PKI Customers using Managed PKI Key Manager.

Symantec's disaster recovery database is synchronized regularly with the production database within the time limits set forth in the Security and Audit Requirements Guide. Symantec's

disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CP/CPS § 5.1.1.

Symantec's disaster recovery plan has been designed to provide full recovery within 24 hours following disaster occurring at Symantec's primary site. Symantec tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at Symantec's primary site as soon as possible following a major disaster.

Symantec maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CP/CPS § 6.2.4.

Symantec maintains offsite backups of important CA information for Symantec CAs as well as the CAs Managed PKI Customers within Symantec's Sub-domain. Such information includes, but is not limited to: application logs, Certificate Application data, audit data (per CP/CPS § 4.5), and database records for all Certificates issued.

4.8.3 Key Compromise

Upon the suspected or known Compromise of a Symantec CA, Symantec infrastructure or Customer CA private key, Symantec's Key Compromise Response procedures are enacted by the Compromise Incident Response Team (CIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other Symantec management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from Symantec executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status in communicated to Relying Parties through the Symantec Repository in accordance with CP/CPS § 4.4.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation of all affected STN Participants, and
- The CA will generate a new key pair in accordance with CP/CPS § 4.7, except where the CA is being terminated in accordance with CP/CPS § 4.9.

4.9 CA Termination

In the event that it is necessary for a Symantec CA or a Managed PKI Customer CA to cease operation, Symantec or the Managed PKI Customer makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, Symantec and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,

- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by Symantec,
- The preservation of the CA's archives and records for the time periods required in CP/CPS § 4.6,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

5. Physical, Procedural, and Personnel Security Controls

Symantec has implemented the Symantec Security Policy, which supports the security requirements of this CPS.

5.1 Physical Controls

5.1.1 Site Location and Construction

Symantec's CA operations are conducted within Symantec's primary facilities in Delaware, which meet the requirements of the Security and Audit Requirements Guide. All Symantec CA and RA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

Symantec's primary facilities have seven physical security tiers with:

- RA validation operations performed within Tier 3
- CA functions performed within Tier 4
- Sensitive servers located in Tier 4
- Online CA cryptographic modules stored in Tier 5
- Offline CA cryptographic modules stored in Tier 7.

Symantec also maintains disaster recovery facilities in California for its CA operations. Symantec's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of Symantec's primary facility.

Managed PKI Customers must ensure that:

- The Managed PKI Customer's site provides appropriate security protection of cryptographic modules, system software and private keys (e.g., the cryptographic module

containing the Managed PKI Administrator's private key should be stored in a secure container or safe when not in use).

- Where a PIN or password is recorded, it must be stored in a security container accessible only to designated personnel.
- RA equipment must be protected from unauthorized access while the cryptographic module is installed and activated.
- Managed PKI Customer employees must not leave their workstations unattended when their private keys are in an unlocked state (i.e., when the PIN or password has been entered).
- Any workstation that contains private keys on a hard drive must be physically secured or protected with an appropriate access control product.
- Hardware cryptographic modules must be physically protected through site protection.
- Physical access controls are implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.
- Security mechanisms must be commensurate with the level of threat in the environment.

5.1.2 Physical Access

Symantec CA systems are protected by four tiers of physical security, with access to the lower tier required before gaining access to the higher tier and using multi-factor authentication. In addition, the physical security system includes three additional tiers for key management security. More information on Symantec's physical security controls can be provided to Customers under a non-disclosure agreement.

5.1.3 Power and Air Conditioning

Symantec's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning (HVAC) systems to control temperature and relative humidity.

5.1.4 Water Exposures

Symantec has taken reasonable precautions to minimize the impact of water exposure to Symantec systems.

5.1.5 Fire Prevention and Protection

Symantec has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Symantec's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within Symantec facilities or in a secure off-site storage facility with appropriate physical

and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with Symantec's normal waste disposal requirements.

5.1.8 Off-Site Backup

Symantec performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and Symantec's disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

Symantec considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of CP/CPS § 5.3.

5.2.2 Number of Persons Required Per Task

Symantec maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA

cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa. Requirements for CA private key activation data and Secret Shares are specified in CP/CPS § 6.2.7.

Other operations such as the validation and issuance of Class 3 Certificates require the participation of at least 2 Trusted Persons.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing Symantec HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in CP/CPS § 5.3.1.

Symantec ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities and
- issued electronic credentials to access and perform specific functions on Symantec CA, RA, or other IT systems.

CA and RA system credentials are:

- directly attributable to an individual;
- not shared; and
- restricted to actions authorized for that role through the use of the CA and RA software.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, Symantec conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records, and
- search of Social Security Administration records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, Symantec will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable personal references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

Symantec provides its personnel with training upon hire and the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily. Symantec periodically reviews and enhances its training programs as necessary.

Symantec's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- Symantec security and operational policies and procedures,

- Security principles and awareness
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Symantec provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Periodic security awareness training is provided on an ongoing basis. Retraining requirements are reviewed periodically and updated as appropriate.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of Symantec policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Contracting Personnel Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a Symantec employees in a comparable position.

Independent contractors and consultants who have not completed the background check procedures specified in CP/CPS § 5.3.2 are permitted access to Symantec's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

Symantec personnel involved in the operation of Symantec's PKI services are required to read this CP/CPS, the STN CP, the Symantec CPS, and the Symantec Security Policy. Such materials are made available through intranet sites. Symantec provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the Security and Audit Requirements Guide. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Symantec Management.

For Symantec RAs, generation of RA key pairs is performed using a cryptographic module certified to FIPS 140-1 level 1. For Managed PKI Administrators, generation of RA key pairs is performed by the RA using a cryptographic module certified to FIPS 140-1 level 2.

Managed PKI Customers generate the key pair used by their Automated Administration servers. Symantec recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is performed by the Subscriber using common Web browser software.

- For SISAC User Individual Basic Certificates Symantec recommends that the end-user Subscriber use a FIPS 140-1 level 1 certified cryptographic module.
- For SISAC User Individual and Organizational Medium Certificates, the end-user Subscriber is required to use a FIPS 140-1 level 1 certified cryptographic service provider.

6.1.2 Private Key Delivery to Entity

End-user Subscriber key pairs are generated by the end-user Subscriber; therefore in such cases, private key delivery to a Subscriber is not applicable.

Where RA key pairs are pre-generated by Symantec on hardware tokens or smart cards, such devices are distributed to the RA using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA using an out of band process. Symantec logs the distribution of such devices.

For Managed PKI Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS # 12 file.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to Symantec for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL).

Where CA, RA, or end-user Subscriber key pairs are generated by Symantec, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Users

Symantec makes the CA Certificates for its PCAs available to Subscribers and Relying Parties through their inclusion in Microsoft and Netscape web browser software. As new PCA Certificates are generated, Symantec provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

Symantec generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. CA Certificates may also be downloaded from the LDAP Directory at *directory.verisign.com*.

6.1.5 Key Sizes

Key pairs shall meet the key length and algorithm requirements specified in Table 11 below.

Entity	*Key Length and Algorithm*
Root CA	2048 bit RSA
Subordinate CA	2048 bit RSA
RA	2048 bit RSA
End-user Subscriber	2048 bit RSA

Table 11 – Key Length and Algorithm Requirements

6.1.6 Public Key Parameters Generation

Not applicable.

6.1.7 Parameter Quality Checking

Not applicable.

6.1.8 Hardware/Software Key Generation

CA, RA and end-user Subscriber key pairs shall be generated in accordance with CP/CPS § 6.2.1.

6.1.9 Key Usage Purposes

Where used for X.509 Version 3 Certificates, Symantec populates the KeyUsage extension of Certificates in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002.

Symantec PCA Certificates are X.509 Version 1 Certificates (see CP/CPS § 7.1.1) and thus do not support the use of the Key Usage extension. For X.509 Version 3 CA Certificates, Symantec uses the Key Usage extension with the keyCertSign and CRLSign bits set and criticality set to false. CA private keys are used only for signing Certificates and CRLs.

For end-user Subscriber Certificates, Symantec may use the Key Usage extension.

6.2 Private Key Protection

Symantec has implemented a combination of physical, logical, and procedural controls to ensure the security of Symantec and Managed PKI Customer CA private keys. Logical and procedural controls are described in CP/CPS § 6.2. Physical access controls are described in CP/CPS § 5.1.2. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Standards for Cryptographic Modules

Key pairs are generated and private keys stored in accordance with Table 12 below.

Entity	*Media*	*Certification Requirement*
CA	Hardware	FIPS 140-1 level 3
RA (Symantec)	Software	FIPS 140-1 level 1
RA (Managed PKI Administrator)	Hardware	FIPS 140-1 level 2
End-user Subscriber (SISAC User Individual and Organizational Medium)	Software	FIPS 140-1 level 1
End-user Subscriber (SISAC User Individual Basic)	Software	None

Table 12 – Standards for Cryptographic Modules

Note: Symantec RA operations are performed within a Tier 3 environment which requires two factor authentication including biometrics as described in CP/CPS § 5.1.1.

6.2.2 Private Key (n out of m) Multi-Person Control

Symantec has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. Symantec uses

"Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (n) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (m) is required to activate a CA private key stored on the module.

Table 13 below shows the threshold number of shared required and the total number of shares distributed for the different types of Symantec CAs. It should be noted that the number of shares distributed for disaster recovery tokens is less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with CP/CPS § 6.4.2.

Entity	*Required Secret Shares to Enable CA's Private Key to Sign End-User Subscriber Certificates*	*Required Secret Shares to Sign CA's Certificate*	*Total Secret Shares Distributed*	*Disaster Recovery Shares*	
				Shares Needed	*Total Shares*
Class 2 PCA	n/a	3	12	3	5
Class 3 PCA	n/a	3	12	3	5
SISAC User Individual Basic CA and subordinate CAs	3	3	12	3	5
SISAC User Individual and Organizational Medium CA and subordinate CAs	3	3	12	3	5

Table 13 – Secret Share Distribution and Thresholds

6.2.3 Private Key Escrow

Symantec does not escrow CA, RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement.

Managed PKI Customers using Managed PKI Key Manager can escrow copies of the private encryption keys of Subscribers whose Certificate Applications they approve. Symantec does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process as described below.

- For each end user key pair backed up, the Managed PKI Key Manager randomly generates a symmetric key used to encrypt the backed up private key at the Customer site. This encrypted private key is then stored in the local database at the Customer site. The symmetric key is also encrypted, using a public key belonging to the Symantec key recovery service, and stored in the local database at the Customer site.
- When an end user's backed up private key must be recovered, the Managed PKI administrator identifies the appropriate key using the key history stored by the Key Manager at the Customer site, and sends the corresponding encrypted symmetric key to the Symantec Recovery Service. The Symantec Key Recovery Service decrypts and returns the symmetric key, which is then used locally to decrypt the end user's private key from the database. This key and the corresponding certificate can then be redistributed to the end user.

Symantec does not escrow end-user Subscriber private signing keys.

6.2.4 Private Key Backup

Symantec creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of CP/CPS § 6.2.1. CA private keys are copied to backup hardware cryptographic modules in accordance with CP/CPS § 6.2.6.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CP/CPS §§ 5.1, 6.2.1. Modules containing disaster recovery copies of CA private keys are subject to the requirements of CP/CPS § 4.8.2.

Symantec does not store copies of RA private keys. Symantec does not store copies of end-user Subscriber private keys except as provided in CP/CPS § 6.2.3.

If the end-user Subscriber creates a backup copy of his or her private key, the backup copy must be safeguarded with a level of protection at least equivalent to that of the primary key.

6.2.5 Private Key Archival

When the CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least five (5) years. Archived CA key pairs will be securely stored using hardware cryptographic modules that meet the requirements of CP/CPS § 6.2.1. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed in accordance with CP/CPS § 6.2.9.

Symantec does not archive copies of RA private keys. Symantec does not archive copies of end-user Subscriber private keys except as provided in CP/CPS § 6.2.3.

6.2.6 Private Key Entry into Cryptographic Module

Symantec generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, Symantec makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Method of Activating Private Key

All Symantec Sub-domain Participants are required to protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.7.1 End-User Subscriber Private Keys

End-user Subscribers are required to:

- Use a password in accordance with CP/CPS § 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, a network logon password; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

6.2.7.2 Administrators' Private Keys

Symantec RAs are required to:

- Use a smart card, biometric access device, or password in accordance with CP/CPS § 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

Managed PKI Administrators are required to:

- Use a cryptographic module along with a PIN or passphrase to authenticate the Administrator before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.7.3 Private Keys Held by Symantec

Symantec CA private keys are activated by a threshold number of Shareholders supplying their activation data (tokens or passphrases) in accordance with CP/CPS § 6.2.2. For Symantec's offline CAs, the CA private key is activated for one session (e.g., for the certification of a Subordinate CA or an instance where a PCA signs a CRL) after which it is deactivated and the module is returned to secure storage. For Symantec's online CAs, the CA private key is activated for an indefinite period and the module remains online in the production data center until the CA is taken offline (e.g., for system maintenance). Symantec Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

6.2.8 Method of Deactivating Private Key

Symantec CA private keys are deactivated upon removal of the CA token from the token reader.

Symantec RA and Managed PKI Administrator private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user.

End-user Subscriber private keys may be deactivated after each operation or upon logging off their system. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with CP/CPS §§ 2.1.3, 6.4.1.

When deactivated, private keys shall be kept in encrypted form only.

6.2.9 Method of Destroying Private Key

At the conclusion of a Symantec's CA's operational lifetime, one or more copies of the CA private key are archived in accordance with CP/CPS § 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

Where required, Symantec destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. Symantec utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Symantec CA, RA and end-user Subscriber Certificates are backed up and archived as part of Symantec's routine backup procedures.

6.3.2 Usage Periods for the Public and Private Keys

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that private keys may continue to be used for decryption and public keys may continue to be used for signature verification. The maximum Operational Periods for Certificates issued on or after the effective date of this CP/CPS are set forth in Table 14 below.

In addition, Symantec CAs stop issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By:	*Class 2*	*Class 3*
PCA to CA	Up to 10 years	Up to 10 years
CA to Subordinate CA	Up to 5 years	Up to 5 years

Certificate Issued By:	*Class 2*	*Class 3*
CA to end-user Subscriber	Normally up to 2 years, but up to 5 years under the conditions described below.	Normally up to 2 years, but up to 5 years under the conditions described below.

Table 14 – Certificate Operational Periods

Except as noted in this section, Symantec Sub-domain Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to five (5) years, if the following requirements are met:

- The Certificates are individual Certificates,
- Subscribers' key pairs reside on a hardware token, such as a smart card,
- Subscribers are annually required to undergo re-authentication procedures under CP/CPS § 3.1.9,
- Subscribers shall annually prove possession of the private key corresponding to the public key within the Certificate,
- If a Subscriber is unable to complete re-authentication procedures under CP/CPS § 3.1.9 successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall automatically revoke the Subscriber's Certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing Symantec CA private keys is generated in accordance with the requirements of CP/CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

Managed PKI Administrators are required to store their Administrator/RA private keys using a FIPS 140-1 level 2 certified hardware cryptographic module protected with a PIN or passphrase.

Symantec RAs and end-user Subscribers are required to select strong passwords to protect their private keys. Symantec's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

6.4.2 Activation Data Protection

Symantec Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

Symantec RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

Managed PKI Administrators are required to safeguard the PIN or passphrase required to activate the hardware cryptographic module containing their Administrator/RA private keys.

End-user Subscribers are required to safeguard the password required to access their private keys. Symantec also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

Symantec performs all CA and RA functions using Trustworthy Systems that meet the requirements of Symantec's Security and Audit Requirements (SAR) Guide. Managed PKI Customers must use Trustworthy Systems that meet the requirements of the Enterprise Security Guide.

6.5.1 Specific Computer Security Technical Requirements

Symantec ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, Symantec limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Symantec's production network is logically separated from other components. This separation prevents network access except through defined application processes. Symantec use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

Symantec require the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. Symantec requires that passwords be changed on a periodic basis.

Direct access to Symantec databases supporting the Symantec Repository is limited to Trusted Persons in Symantec's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

A version of Symantec's core Processing Center software has satisfied the EAL 4 assurance requirements of ISO/IEC 15408-3:1999, *Information technology - Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*, based on an independent laboratory's Common Criteria evaluation of the software against the Symantec Processing Center Security Target. Symantec may, from time to time, evaluate new releases of the Processing Center software under the Common Criteria.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by the Symantec in accordance with Symantec systems development and change management standards. Symantec also provides software to its Managed PKI Customers for performing RA and certain CA functions. Such software is developed in accordance with Symantec system development standards.

Symantec developed software, when first loaded, provides a method for to verify that the software on the system originated from Symantec, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

Symantec has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Symantec creates a hash of all software packages and Symantec software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, Symantec validates the integrity of its CA systems.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Symantec performs its CA and RA functions using networks secured in accordance with the Security and Audit Requirements Guide to prevent unauthorized access and other malicious activity. Symantec protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Cryptographic Module Engineering Controls

Cryptographic modules used by Symantec meet the requirements specified in CP/CPS § 6.2.1.

7. Certificate and CRL Profile

7.1 Certificate Profile

CP/CPS § 7.1 defines Symantec's Certificate Profile and Certificate content requirements for STN Certificates issued under this CPS.

Symantec Certificates conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280").

At a minimum, Symantec X.509 Certificates contain the basic X.509 Version 1 fields and indicated prescribed values or value constraints in Table 15 below:

Field	*Value or Value constraint*
Version	See CP/CPS §7.1.1.
Serial Number	Unique value per Issuer DN
Signature Algorithm	Name of the algorithm used to sign the certificate (See CP/CPS § 7.1.3)
Issuer DN	See CP/CPS § 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280. The validity period will be set in accordance with the constraints specified in CP/CPS § 6.3.2.
Subject DN	See CP/CPS § 7.1.4
Subject Public Key	Encoded in accordance with RFC 3280 using algorithms specified in CP/CPS § 7.1.3 and key lengths specified in CP/CPS § 6.1.5.
Signature	Generated and encoded in accordance with RFC 3280

Table 15 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

Symantec CA and end-user Subscriber Certificates are X.509 Version 3 Certificates with the exception of the Symantec PCAs which are X.509 Version 1 Certificates.

7.1.2 Certificate Extensions

Where X.509 Version 3 Certificates are used, Symantec populates Certificates with the extensions required by CP/CPS §§ 7.1.2.1-7.1.2.8. Private extensions are permissible as long as their use is consistent with the STN CP and this CP/CPS.

7.1.2.1 Key Usage

Symantec uses the KeyUsage extension in accordance with CP/CPS § 6.1.9.

7.1.2.2 Certificate Policies Extension

Symantec X.509 Version 3 end-user Subscribers Certificates use the Certificate Policies extension. The CertificatePolicies extension is populated with the applicable object identifier specified in CP/CPS §1.2 in accordance with CP § 7.1.6 and with policy qualifiers set forth in CP § 7.1.8. The criticality field of this extension is set to FALSE.

7.1.2.3 Subject Alternative Names

No stipulation.

7.1.2.4 Basic Constraints

Symantec populates X.509 Version 3 CA Certificates with a BasicConstraints extension with the Subject Type set to CA. X.509 Version 3 CA Certificates set the "pathLenConstraint" field to a value representing the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to the online CAs of Managed PKI Customers and Symantec CAs, issuing end-user Subscriber Certificates, set the "pathLenConstraint" field to a value of "0" indicating that only an end-user Subscriber Certificate may follow in the certification path.

End-user Subscriber Certificates are also populated with a BasicConstraints extension with the Subject Type equal to End Entity. The criticality of the Basic Constraints extension is generally set to FALSE. The criticality of this extension may be set to TRUE for other Certificates in the future.

7.1.2.5 Extended Key Usage

No stipulation.

7.1.2.6 CRL Distribution Points

Symantec X.509 Version 3 Certificates use the CRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

No stipulation.

7.1.2.8 Subject Key Identifier

No stipulation.

7.1.2.9 authorityInfoAccess Extension

Should we say something since Symantec offers OCSP?

7.1.3 Algorithm Object Identifiers

Symantec X.509 Certificates are signed with sha1RSA (OID: 1.2.840.113549.1.1.5) or md5RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 3280.

7.1.4 Name Forms

Symantec populates STN Certificates with an Issuer and Subject Distinguished Name in accordance with CP/CPS § 3.1.1.

In addition, Symantec includes within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement are permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in CP/CPS § 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Symantec populates X.509 Version 3 STN Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the Symantec CPS. In addition, some Certificates contain a User Notice Qualifier that points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

Symantec issues CRLs that conform to RFC 3280. At a minimum, Symantec CRLs contain the basic fields and contents specified in Table 16 below:

Field	*Value or Value constraint*
Version	See CP/CPS §7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. CRLs are signed using md5RSA (OID: 1.2.840.113549.1.1.4) or md2RSA (OID: 1.2.840.113549.1.1.2) in accordance with RFC 3280.
Issuer	Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in CP/CPS § 7.1.4.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. The Next Update date for CRLs is set as follows: 3 months from the Effective Date for PCAs and 10 days from the Effective Date for other CAs. CRL issuance frequency is in accordance with the requirements of CP/CPS § 4.4.9.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 16 – CRL Profile Basic Fields

7.2.1 Version Number(s)

Symantec currently issues X.509 Version 1 CRLs and will support the issuance of X.509 Version 2 CRLs in the future.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8. Specification Administration

8.1 Specification Change Procedures

Amendments to this CP/CPS shall be made by the Symantec Practices Development group. Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the Symantec Repository located at: *http://www.symauth.com/repository/*. Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS.

8.1.1 Items that Can Change Without Notification

Symantec reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. Symantec's decision to designate amendments as material or non-material shall be within Symantec's sole discretion.

8.1.2 Items that Can Change with Notification

Symantec shall make material amendments to the CPS in accordance with this CP/CPS § 8.1.2.

8.1.2.1 List of Items

Material amendments are those changes that Symantec, under CP/CPS § 8.1.1, considers to be material.

8.1.2.2 Notification Mechanism

Symantec's Practices Development group will post proposed amendments to the CPS in the Practices Updates and Notices section of the Symantec Repository, which is located at: *http://www.symauth.com/repository/*. Symantec solicits proposed amendments to the CPS from other Symantec Sub-domain Participants. If Symantec considers such an amendment desirable and proposes to implement the amendment, Symantec shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if Symantec believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the STN, Symantec's Sub-domain, or any portion of the STN, Symantec shall be entitled to make such amendments by publication in the Symantec Repository. Such amendments will be effective immediately upon publication.

8.1.2.3 Comment Period

Except as noted under CP/CPS § 8.1.2.2, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the Symantec Repository. Any Symantec Sub-domain Participant shall be entitled to file comments with Symantec's Practices Development group up until the end of the comment period.

8.1.2.4 Mechanism to Handle Comments

Symantec's Practices Development group will consider any comments on the proposed amendments. Symantec will either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment under CP/CPS § 8.1.2.2, or (c) withdraw the proposed amendments. Symantec is entitled to withdraw proposed amendments by providing notice in the Practices Updates and Notices section of the Symantec Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period under CP/CPS § 8.1.2.3.

8.1.3 Changes Requiring Changes in the Certificate Policy OID or CPS Pointer

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

8.2 Publication and Notification Policies

8.2.1 Items Not Published in the CP/CPS

Security documents considered confidential by Symantec are not disclosed to the public. Confidential security documents include the documents identified in CP/CPS § 1.1(a) as documents that are not available to the public.

8.2.2 Distribution of the CP/CPS

This CP/CPS is published in electronic form within the Symantec Repository at *http://www.symauth.com/repository/*. Symantec also makes the CP/CPS available upon request sent to *practices@symantec.com*. Requests may be sent to: Symantec Corporation, 350 Ellis Rosd, Mountain View, CA 94043 USA, Attn: Practices Development – CP/CPS.

8.3 CP/CPS Approval Procedures

Modifications to this CP/CPS shall be approved by the Symantec Practices Development group upon receiving review and approval from SISAC.

Acronyms and Definitions

Table of Acronyms

Acronym	Term
ANSI	The American National Standards Institute.
B2B	Business-to-business.
CA	Certification Authority.
CP	Certificate Policy.
CPRD	Mortgage Bankers Association - Secure Identity Services Accreditation Corporation Certificate Policy Requirements Document
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
MBA	Mortgage Bankers Association of America
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
SISAC	Secure Identity Services Accreditation Corporation
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
STN	Symantec Trust Network.

Definitions

Term	Definition
Administrative Certification Authority (Administrative CA)	A type of Symantec CA that issues Certificates to Symantec RAs, Managed PKI Customer personnel (Managed PKI Administrators), and Automated Administration servers.
Administrator	A Trusted Person within Symantec or the organization of a Managed PKI Customer that performs validation and other CA or RA functions.

Term	Definition
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with Symantec to be a STN distribution and services channel within a specific territory.
Affiliated Individual	A natural person that is related to a given entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a Symantec registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by Symantec that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	The document entitled "Symantec Trust Network Certificate Policies" and is the principal statement of policy governing the STN.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the STN.
Certification Practice Statement (CPS)	A statement of the practices that Symantec employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers to employ. In the context of this document, "CPS" refers to the Symantec Certification Practices Statement.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.

Term	Definition
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1. The distinctions are summarized in CP/CPS § 1.1.1.
Client OnSite Customer	See Managed PKI Customer.
Compliance Audit	A periodic audit that Symantec or a Managed PKI Customer undergoes to determine its conformance with STN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP/CPS § 2.8.1.
Customer	An organization that is a Managed PKI Customer.
Enterprise Security Guide	A document setting forth security requirements and practices for Managed PKI Customers.
Exigent Audit/Investigation	An audit or investigation by Symantec where Symantec has reason to believe that an entity's failure to meet STN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the STN posed by the entity has occurred.
Go Secure!	A suite of plug-and-play services building on Managed PKI services and designed to accelerate e-commerce applications.
Infrastructure Certification Authority (Infrastructure CA)	A type of Symantec CA that issues Certificates to components of the Symantec infrastructure supporting certain Symantec services. Infrastructure CAs do not issue CA, RA, or end-user Subscriber Certificates.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Ceremony Reference Guide	A document describing Key Generation Ceremony requirements and practices.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Client Managed PKI Customer using Managed PKI Key Manager.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A Symantec service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.

Term	Definition
Managed PKI	Symantec's fully integrated managed PKI service that allows enterprise Customers of Symantec to distribute Certificates to individuals, such as employees, partners, suppliers, and customers. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for a Managed PKI Customer.
Managed PKI Administrator Handbook	A Symantec document setting forth the operational requirements and practices for Managed PKI Customers.
Managed PKI Agreement	An agreement under which an organization becomes a Managed PKI Customer and agrees to be bound by this CPS.
Managed PKI Certificate	A Certificate whose Certificate Application was approved by a Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications.
Managed PKI Customer	An organization that has obtained Managed PKI services from Symantec, whereby the organization becomes a CA within the STN to issue client Certificates. Managed PKI Customers outsource back-end functions of issuance, management, and revocation to Symantec, but retain for themselves the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Manager Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.

Term	Definition
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within Symantec responsible for promulgating this policy throughout the STN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (Symantec or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the STN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The STN PKI consists of systems that collaborate to provide and implement the STN.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by Symantec, acting as CA, to individuals or organizations applying one by one to Symantec on its web site.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP/CPS § 6.2.2.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements Guide	An internal Symantec document that sets forth the security and audit requirements and practices for Processing Centers.
SISAC User Individual Basic	As defined by SISAC, this assurance level is relevant to environments where the risks and consequences of data compromise are not considered by the Certificate Holder/Subscriber to be of major significance. This may include access to private information where the likelihood of malicious access is not high.

Term	Definition
SISAC User Individual and Organizational Medium	As defined by SISAC, this assurance level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
Subdomain	The portion of the STN under control of an entity and all entities subordinate to it within the STN hierarchy.
Subject	The holder of a private key corresponding to a public key. . A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a STN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by Symantec following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Symantec Security Policy	The highest-level document describing Symantec's security policies.
Symantec Subdomain Participants	An individual or organization that is one or more of the following within the Symantec's Subdomain of the STN: Symantec, a Customer, a Subscriber, or a Relying Party.
Trusted Person	An employee, contractor, or consultant of an entity within the STN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP/CPS § 5.2.1.
Trusted Position	The positions within a STN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Symantec Repository	Symantec's database of Certificates and other relevant Symantec Trust Network information accessible on-line.
Symantec Security Policy	The highest-level document describing Symantec's security policies.
Symantec Subdomain Participants	An individual or organization that is one or more of the following within the Symantec's Sub-domain of the STN: Symantec, a Customer, a Subscriber, or a Relying Party.
Symantec Trust Network (STN)	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 respective Customers, Subscribers, and Relying Parties.

Term	Definition
STN Participant	An individual or organization that is one or more of the following within the STN: Symantec, a Customer, a Subscriber, or a Relying Party.
STN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the STN.

Appendix A: History of Changes

History of changes: version 1.3

Section	Description
Throughout document	Changes to identify the Symantec Trust Network (STN) brand and Symantec network URL addresses.

History of changes: version 1.2

Section	Description
Throughout document	Changes to identify Symantec Corporation acquisition & owner of the VTN CA services.
1.1.1.3, 5.1 & 6.2.7 & Appendix A	Removed VeriSign Roaming Service which is EOL.
2.4.1, 2.4.3, 2.3.1 & 2.8	Changes to Governing Law, Assets & Privacy Plan in accord with Symantec ownership.

History of changes: version 1.1

Section	Description
Sections 2.4.1 and 2.4.3.2	Governing Law jurisdictions changed from New York & California to Fairfax Country Virginia.
Section 5.1.1 – Site Location	Changed location of Primary site from MV CA to Delaware and DRF from Virginia to Mountain View, California.