Symantec Gatekeeper
General Category Certificate Policy

General Category Business and Individual Certificates
and
General Supplementary Device Certificates

Version 2.0

25 September 2013

Symantec Gatekeeper General Category Certificate Policy

Published date: September 25, 2013

Trademark Notices

TABLE OF CONTENTS

1. INTRODUCTION

Symantec (Australia) Pty Ltd trading as Symantec Gatekeeper Services ('Symantec') provides both Public and Private certification services using technology from Symantec Corporation. Symantec Corporation, headquartered in Mountain View, California, is the largest maker of security software for computers, a Fortune 500 company and a member of the S&P 500 stock market index. Symantec's User Authentication solutions provide convenient, secure fraud detection, two-factor authentication and public key infrastructure (PKI) services for protecting online identities and interactions between consumers, business partners, and employees.

The Symantec Gatekeeper Certificate Policy ("CP") sets out a number of policy and operational matters for the issuance of Gatekeeper X.509 v3 compliant **General Category** Certificates as defined in the Gatekeeper PKI Framework developed by the Department of Finance and Deregulation, through the Australian Government Information Management Office (AGIMO). The Gatekeeper Competent Authority approves the Symantec Gatekeeper Accreditation. Information about the AGIMO can be found at *www.finance.gov.au/e-government/index.html*. Information describing the Gatekeeper PKI Framework can be found at *www.gatekeeper.gov.au*

This CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates for the Symantec Gatekeeper PKI. The Symantec Gatekeeper PKI issues digital certificates under the Gatekeeper PKI Framework. These digital certificates provide authentication, confidentiality, integrity and non-repudiation in transactions. These certificates meet the x.509 standards and accommodate inclusion of the Australian Business Number (ABN) as appropriate.

Digital certificates issued under the **General Category** are issued to individuals, organisations and devices for the purpose of conducting online transactions with government agencies. The General Category includes x.509 compliant Identity Certificates for both an Individual and an Organisation as well as x.509 compliant Supplementary Certificates, specifically the Supplementary Device Certificates, that contain specialised extensions and used to identify and authenticate applications or devices that are owned and/or operated by an organisation.

The Symantec Gatekeeper PKI under the General Category is regarded as "open" in that digital certificates issued may be relied upon by multiple Agencies without the necessity for contractual arrangements between them and the Issuing CA. Notwithstanding, the Symantec Gatekeeper PKI also establishes contractual relationships with Organisations and their Subscribers enrolled for certificate services.

This Certificate Policy (CP) covers only those matters specific to the General Category Certificate including the obligations of the PKI Entities, as identified in section 1.3. The obligations of the PKI End Entities are also set out in the relevant Subscriber Agreement and Relying Party Agreement. The Certification Authority (CA) PKI Entities are constituted in a two level hierarchy whereby the top Root CA level of the hierarchy possesses unique functions and obligations separate from the lower Issuing CA level. As such, the common functions and obligations of all Issuing CAs are addressed within the body of this CP while those of the top level Root CA are identified separately in Appendix D. For more information about Symantec's detailed practices as a Certification Authority (CA) refer to the Symantec Gatekeeper Certification Practice Statement (CPS).

The structure of this CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. Expressions used in this CP are defined in the Glossary which can be found on the Symantec Gatekeeper Website*: https://symantec-gatekeeper.com.au/repository/.*

The provisions of Symantec Gatekeeper CP supersede the provisions of the Symantec Gatekeeper CPS in the event of any direct inconsistency.

1.1 Overview

The Symantec Gatekeeper General Category CP describes a two level PKI hierarchy consisting of a Trusted Root and two types of subordinate Issuing CAs as depicted in the following diagram (figure 1). In this hierarchy the Root CA is a single top level CA only. At the subordinate level, one instance of each type of Issuing CA shall be created for the issuance of end-entity certificates.

In this CP, the term "Symantec Gatekeeper CA", also abbreviated as "Symantec CA", refers to an Issuing CA within the PKI hierarchy providing the Symantec Gatekeeper CA services (inclusive of the combined systems, personnel and processes that perform the functions and provide the services of the PKI).

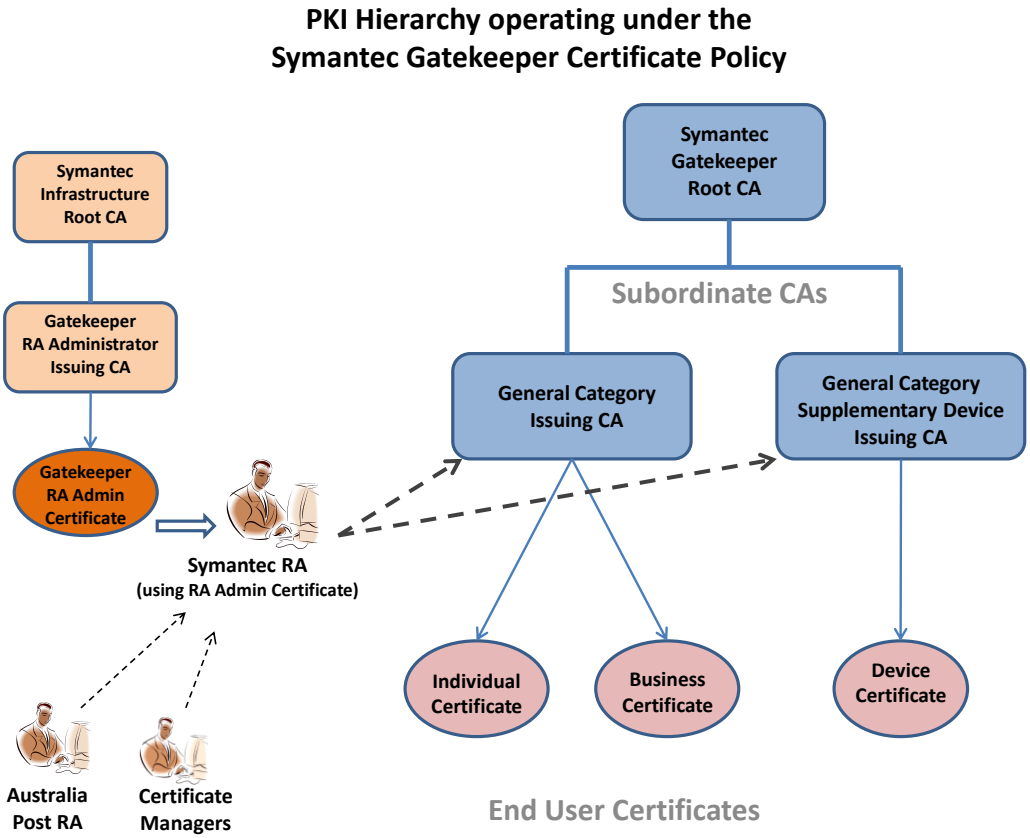

Figure 1: Symantec Gatekeeper PKI Hierarchy

The Symantec Gatekeeper PKI supports the General Category Individual and Business Certificates ("Individual" and "Business") as well as the General Supplementary Device Certificates ("Device").

Certificates in the General Category are issued under a range of Evidence of Identity (EOI) models and will be distinguished on the basis of the EOI model and level/type of EOI assurance underpinning the issue of a digital certificate. The Symantec Gatekeeper General Category PKI supports the following three EOI Models:

- **Formal Identity Verification Model** – under this model all applicants undergo a face-to-face EOI check in the presence of an accredited Registration Authority (RA).
- **Known Customer Organisation (KCO) Model** – the Symantec Gatekeeper CA may issue certificates to clients of an Organisation or Agency that is Gatekeeper Listed by the Gatekeeper Competent Authority under this model of identity verification.
- **Independent Threat and Risk Assessment (TRA) Model** –the Symantec Gatekeeper CA may issue certificates to clients of an Organisation or Agency that is Gatekeeper Listed by the Gatekeeper Competent Authority under this model of identity verification.

The policy for the KCO and the TRA Models is described in Appendix E of this CP.

Two types of Certificates are issued under this Certificate Policy for **Individual and Business Certificates**:

a) Certificates used for Signing; and
b) Certificates used for Encryption.

One Certificate issued under this Certificate Policy for **Device Certificates** can be used for both Signing and Encryption.

The **Gatekeeper Individual Certificate** is used to identify an individual acting in his/her private capacity. An Individual Certificate identifies an individual (as a Key Holder) for the purpose of conducting online/electronic transactions with government agencies in a secure manner. The Individual Certificate shall assert within a certificate extension, the model of Evidence of Identity (EOI) that is used in Subscriber identity verification.

The **Gatekeeper Business Certificate** is used to identify a person (as Key Holder) as an employee or representative of an Organisation for the purpose of Organisations conducting online transactions with government agencies. The term 'business' is inclusive of all non-individual entities (organisations) whether or not the entity has an Australian Business Number (ABN), however, the Business certificate allows for inserting an ABN into a Certificate Extension in the Certificate.

The Business Certificate shall include the Organisation's legal name and optionally the Organisation's trading name(s). The Business Certificate shall assert within certificate extensions, the model and assurance type of EOI that is used for Subscriber identity verification. The EOI assurance type distinguishes to a Relying Party whether the Key Holder holds a Certificate Manager or an Additional Key Holder role for the Organisation.

Symantec Gatekeeper distinguishes two variations of the Business certificate based upon the EOI assurance type: the ***Standard Business Certificate*** identifies the Key Holder as an Additional Key Holder and the ***Gatekeeper Manager Certificate*** identifies the Key Holder as a Certificate Manager.

The **Gatekeeper Device Certificate** is used to identify an application, device, process or service that is owned, operated or controlled by an Organisation for the purposes of transacting with other organisations and agencies. A Device Certificate may be installed on a Device to enable an Organisation to:

a) digitally sign communications from an Organisation (eg, an email auto-responder, an email generated by a software process, or an electronic data interchange (EDI) software client); or
b) encrypt communications sent to an Organisation (eg when email is sent to a generic drop mail box or to an EDI server/client).

Device certificates contain specified elements and certificate extensions that are used to identify and authenticate applications or devices (including a process or service) that are owned and/or operated by an Organisation. An individual within the organisation is required to take responsibility for the Device certificate however, he/she is not named in the Device certificate.

The request for a Device Certificate shall identify the Certificate Manager (individual) responsible for managing the Device Certificate on behalf of the Organisation. This individual is not named within the certificate.

1.2 Document Name and Identification

This CP is known as the "Symantec Gatekeeper Certificate Policy". The following OIDs correspond to the Symantec Gatekeeper Certificate Policy:

General Category Policy 1.2.36.88021603.333.20.1

CAs operating under this Certificate Policy may issue Subscriber certificates including:

General Category Individual Certificates
General Category Business Certificates
General Supplementary Device Certificates

1.3 PKI Participants

1.3.1 Certification Authorities

The Certification Authorities (CA) that issues Certificates under this CP are the Symantec Gatekeeper Root CA–G2 and its Subordinate CA's operated by Symantec (Australia) Pty Ltd. The Root CA issues CA Certificates to a Subordinate CA and the Subordinate CA issues end entity Certificates to Subscribers.

The Root CA and Subordinate CAs uniformly assume the functions and obligations of CAs as outlined in this CP and the corresponding CPS. However, the Root CA also assumes additional functions and obligations that are distinct for the Root CA alone as outlined in Appendix D of this CP.

1.3.2 Registration Authorities

The Symantec RA or another Gatekeeper Accredited RA as an RA Service Provider will perform the functions of the Registration Authority.

When an RA functioning under this CP is performed by a Gatekeeper Accredited RA other than the Symantec RA, that RA will be bound contractually by Symantec to perform the Registration functions, in accordance with this CP and other Approved Documents.

Under the Formal identity Verification Model, the RA shall verify the identity and the bindings of Subscribers through a face-to-face EOI check as stipulated in section 3.2. Identity verification shall verify the binding of the physical person to the documented name of the Subscriber or Key Holder. Organisation verification shall verify the identity of the Organisation and bind the individual named in the Certificate to the Organisation. The Symantec RA shall perform the identity verification of the Subscriber of the Business and Device Certificates (i.e, Organisation). A Gatekeeper accredited Registration Authority shall perform the identity verification of the Subscriber of the Individual and the Certificate Manager Certificates (ie, individuals). The Certificate Manager serves as a delegated RA as described in section 1.3.4.2.

The Symantec RA is granted privileged access to the CA. Gatekeeper accredited RAs and delegated RAs are not granted privileged access to the CA.

Also refer to Appendix E for a description of the RA function under additional EOI Models. The RA shall supply the correct indication of EOI model and EOI assurance type conducted in identity verification for insertion into the certificate.

1.3.3 End Entities

The End Entities to which this CP applies are Subscribers and Relying Parties.

1.3.3.1 Subscribers

A Subscriber is an entity whose name appears as the subject in a digital certificate issued by the Gatekeeper-accredited CA, and who asserts that it uses its keys and certificate in accordance with the Symantec Gatekeeper General Category CPS. This Certificate Policy is applicable to the following Subscribers.

- Subscribers of the Gatekeeper **Individual Certificate** are individuals acting in their private capacity wishing to conduct online transactions with government agencies.
- Subscribers of the Gatekeeper **Business Certificate** are organisations (ie, non-individual entities) wishing to conduct online transactions with government agencies. The holder of the Business Certificate represents the Organisation in electronic transactions and is also referred to as a Key Holder.
- Subscribers of the Gatekeeper **Device Certificate** are organisations wishing to conduct online transactions with government agencies. Such organisations may do so via devices/applications/servers.

In terms of registration, the term “applicant” refers to the person who generates the request and enters the details to appear in a Certificate.

1.3.3.2 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the Symantec Gatekeeper PKI. A Relying party may, or may not also be a Subscriber within the Symantec Gatekeeper PKI.

1.3.4 Other Participants

1.3.4.1 Authoriser

An Authoriser is a member of a class of persons with a clear capacity to commit an Organisation and to appoint a Certificate Manager to act on behalf of the Organisation only with respect to application for and management of digital certificates. Persons who are members of this class include (but are not limited to):

a) Chief Executive Officer;
b) Company Director;
c) Trustee;
d) Partner; or
e) Company Owner.

A Business Entity which intends to authorise the use of Device Certificates must have at least one Authoriser. The Authoriser's authority to perform their duties is evidenced in accordance with section 3.2.6.

An Authoriser appoints an individual with the authority to fulfill the role of Certificate Manager acting as a Delegated RA on behalf of the Organisation.

1.3.4.2 Certificate Manager

A Certificate Manager is authorised to act on behalf of an Organisation and performs delegated RA tasks for the provisioning of digital certificates within the Organisation.

An Organisation may have one or more Certificate Managers. A small Organisation may have only one Certificate Manager while a large or decentralised Organisation may choose to appoint a number of Certificate Managers for practical operational purposes. Given the critical role played by the Certificate Manager in the issuance of Certificates for an Organisation, the allocation of such positions shall be strictly managed by the Organisation.

The Certificate Manager role and the person providing the Certificate Manager with that authority (the Authoriser) may be one and the same person, particularly in a small Organisation.

A person appointed by the Organisation as a Certificate Manager cannot appoint other Certificate Managers unless the person is also an Authoriser.

A Certificate Manager shall use a Symantec Gatekeeper Manager Certificate for authentication to perform their duties and as such is the Subject/Key Holder of the Symantec Gatekeeper Manager Certificate who accepts the Subscriber Agreement prior to receipt of the Gatekeeper Manager Certificate. The Certificate Manager's authority to perform their duties is evidenced in accordance with section 3.2.6.

1.3.4.2.1 Responsibilities in Business Certificate Issuance

A Certificate Manager is a duly authorised member (e.g., employee, contractor or otherwise engaged by an organisation) of an Organisation who has been issued with a Symantec Gatekeeper Manager Certificate for the purposes of obtaining and managing additional digital certificates for other employees of the Organisation.

The Certificate Managers has the authority to undertake the application and request issuance of additional Business Digital Certificates directly with the Symantec Gatekeeper CA using their Symantec Gatekeeper Manager Certificates to authenticate themselves to the CA.

The Certificate Manager is authorised by the Organisation as responsible to:

1. To submit an application under the Delegated RA process to hold a Business Certificate on behalf of the Organisation;
2. complete, sign and lodge the necessary documentation that provide EOI of the Organisation and the Certificate Manager;
3. under the Delegated RA process, request additional Business Certificates for the Organisation as required for use by other representatives of the Organisation;
4. undertake the obligations set out in section 9.6.3.3 on behalf of the Organisation.

1.3.4.2.2 Responsibilities in Device Certificate Issuance

The Certificate Manager is an individual who has been given responsibility for requesting, accepting, installing and managing Device Certificates on behalf of an Organisation.

The Certificate Manager is authorised by the Organisation as responsible to:

1. hold a Symantec Gatekeeper Manager Certificate on behalf of the Organisation;
2. request Device Certificates for the Organisation as required; and
3. undertake the obligations set out in section 9.6.3.3 on behalf of the Organisation.

The Certificate Manager role shall perform the following functions:

1. Accurately identify and locate devices/applications upon which Device Certificates are to be installed.
2. Request issuance of certificates as required
   - Submit an application for a Device Certificate; and
   - request additional Device Certificates as required for use by the Organisation.
3. Accept device keys and certificates on behalf of the Organisation
4. Ensure that device keys and certificates are installed on the identified device/application, and
5. Manage devices / applications
   - manage the lifecycle of Device Certificates on devices/applications within the Organisation, and
   - maintain the security of device keys and certificates within the Organisation.

1.3.4.3 Policy Management Authority

The Symantec Gatekeeper Policy Management Authority (PMA) is responsible for maintaining this CP, approving the corresponding CPS and enforcing the performance of the Compliance Audit for each CA that issues certificates under this CP as depicted in the PKI hierarchy in section 1.1. In developing the content of this CP, the Symantec Gatekeeper PMA addresses the requirements of the Gatekeeper Competent Authority.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The purpose of the subordinate Issuing CA Certificates and Key Pairs issued under this CP is to sign end-entity Certificates and Certificate status responses for the Certificates issued.

The purpose of the end-entity Certificates and Key Pairs issued under this CP is to facilitate electronic transactions with, and on behalf of, Agencies and others, and more particularly to enable a Subscriber to:

a) authenticate itself to a Relying Party electronically in online transactions;
b) digitally sign electronic documents, transactions and communications; and
c) confidentially communicate with a Relying Party.

A Business or Individual Certificate is suitable for supporting the transmission of information from Unclassified up to and including information bearing Sensitive DLMs, except Sensitive: Cabinet as defined by an agency in accordance with the Australian Government Protective Security Policy (PSPF).

The use of Symantec Gatekeeper Certificates for transactions containing sensitive information (eg, In Confidence or Highly Protected Status) may be restricted by the individual transacting parties as desired.

1.4.2 Prohibited Certificate Uses

Symantec's services under this CP and the corresponding CPS are not designed, intended, or authorised 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.

Symantec has specifically limited its liability in respect of Symantec Gatekeeper Certificates as specified in section 9.8 of this CP.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

Symantec Australia Pty. Ltd. (A wholly owned subsidiary of Symantec Corporation)
ABN: 59 085 397 100
134 Moray St.
South Melbourne, Victoria

Phone: +61 3 9674 5500
Fax: +61 3 9674 5574

1.5.2 Contact Person

Enquiries in relation to this CP should be directed to:

PKI Policy Manager
Symantec Gatekeeper Policy Management Authority
c/o Symantec Australia Pty. Ltd. (A wholly owned subsidiary of Symantec Corporation)
134 Moray St.
South Melbourne, Victoria
Phone: +61 3 9674 5500
Fax: +61 3 9674 5574
practicesGK@symantec.com

1.5.3 Person Determining CPS Suitability for the Policy

The Symantec Gatekeeper Policy Management Authority (PMA) is the final authority that determines the suitability and applicability of the Symantec Gatekeeper CPS for this Policy. While Symantec Corporation is a global company, the PMA members responsible for the Symantec Gatekeeper PKI services are located in Australia.

1.5.4 CP Approval Procedures (Gatekeeper Accreditation)

The Gatekeeper Competent Authority is responsible for approving this CP and any subsequent changes for compliance with Gatekeeper Accreditation Criteria and granting Gatekeeper Accreditation. The Symantec Gatekeeper Policy Management Authority (PMA) is responsible for maintaining this CP document for accuracy and compliance and to provide revised documents to the Gatekeeper Competent Authority for subsequent approval.

The Symantec RA has been granted Gatekeeper Accreditation to verify the identity of organisations, and the Symantec Gatekeeper CA for the issuance of General Category Individual and Business Certificates and General Supplementary Device Certificates under this CP, and perform the other functions specified in this CP, in accordance with this CP.

1.6 Definitions and Acronyms

See Appendix A for a list of acronyms and definitions used throughout this document.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Symantec shall operate standard X.500 directory services in accordance with ITU-T Recommendation X.500 (also known as ISO/IEC 9594: Information Technology -- Open Systems Interconnection -- The Directory).

2.2 Publication of Certification Information

The Symantec CA shall make the Symantec Gatekeeper Root (SGR) Certificate and the SGR Public Key available to End Entities via the Symantec Gatekeeper Repository.

The Symantec CA shall maintain the Symantec Gatekeeper Website at which it publishes or links to:

- the Repository and Certificate Directory;
- the Certificate Revocation List (CRL);
- this CP and the corresponding CPS, and
- Subscriber and Relying Party Agreements.

2.3 Time or Frequency of Publication

CA and End Entity Certificate information is published promptly after it is made available to the CA.

Certificate status information is published in accordance with section 4.9.7 (CRLs) and section 4.9.9 (OCSP).

Updates to this CP and CPS documents are published in accordance with Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary.

2.4 Access Controls on Repositories

Read only access is provided to this CP, the CPS, and other Approved Documents such as the Subscriber Agreement and Relying Party Agreement, in the Symantec Repository.

Access to the Certificate Directory and the CRL is limited to single searches on the following fields as defined in the relevant Certificate Profile: Common Name and email address.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The Symantec CA shall assign a Distinguished Name (DN) to a Subscriber based on the Registration information submitted for a specific Certificate Type. The DN included in the certificate "Subject" field shall be constructed in accordance with the following attribute types:

			Certificate Types		
Standard Attribute Type	**Value**	**Example**	**Individual**	**Business**	**Device**
Email Address (E)	Email	*E = jsmith@widgets.com.au*	Yes	Yes	No
Common Name (CN)	Subscriber/Key Holder name, OR Application/Device name	*CN = John Smith, or CN = CCF Email Gateway (Device)*	Yes	Yes	Yes
Organisational-unit (optional) (OU)	"Encryption Certificate" or "Signing Certificate"	*OU = Signing Certificate*	Yes	Yes	No
Organisational-unit (optional) (OU)	Business unit	*OU = Finance Dept*	No	Yes	Yes
Organisation (O)	Legal Entity Name	*O = Widgets Co. Pty Ltd*	No	Yes	Yes
Location (optional) (L)	Location	*L = Melbourne*	Yes	Yes	Yes
State or Province (S)	State	*S = NSW*	Yes	Yes	Yes
Country (C)	Australia	*C = AU*	Yes	Yes	Yes

Table 1: Distinguished Name Attributes in End User Subscriber Certificates

The Symantec CA may refuse to assign a DN based on the registration information on reasonable grounds, for example where the DN is considered to:

a) be obscene or offensive;
b) mislead or deceive Relying Parties (including where the pseudonym has already been issued to an individual);
c) infringe the IP Rights of any person; or
d) otherwise be contrary to law.

3.1.2 Need for Names to be Meaningful

DNs that are created based on authenticated Evidence of Identity (EOI) are assumed to be meaningful. In the case of Device certificates, EOI is not authenticated and the DNs are created based on information provided in the application and assumed to be meaningful to the Organisation.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous Certificates are not supported.

In the case of Business certificates, with the consent of the Organisation, applicants may apply for a Certificate which incorporates a pseudonym. It is the responsibility of the Organisation to ensure that the pseudonym is meaningful to the Organisation.

3.1.4 Rules for Interpreting Various Name Forms

DNs must include each of the elements specified in the relevant X.509-compliant Certificate Profile.

3.1.5 Uniqueness of Names

The Subject DN allocated by the Symantec CA will be unique to that Certificate Type. This is enforced by the software operated by the Symantec CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

Trademark rights or other IP Rights may exist in the Organisation's name, or other parts of the Registration Information or Certificate Information.

By applying for Registration, the Subscriber, Certificate Applicant and the organisation:

a) authorise the Symantec CA, Symantec RA and Gatekeeper Accredited RAs to use the relevant Intellectual Property for the purpose of creating a Distinguished Name and for other purposes reasonably necessary in relation to issue of Keys and Certificates to, and their use by, the Subscriber or the Organisation and its Subscribers;

b) warrant that they are entitled to use that Intellectual Property for the purposes for which Keys and Certificates are issued and may be used, without infringing the rights of any other person; and

c) agree to indemnify the Symantec CA, Symantec RA and Gatekeeper Accredited RAs , and their respective officers, employees, contractors and agents against loss, damage, costs or expenses of any kind (including legal costs on a solicitor-client basis) incurred by them in relation to any claim, suit or demand in respect of an infringement or alleged infringement of the IP Rights of any person.

The Symantec CA does not independently check the status of any trademark or other IP Rights.

3.1.7 Name Claim Dispute Resolution

Disputes regarding assignment of Distinguished Names must be resolved under section 9.13.

3.2 Initial Identity Validation

Under the Formal Identity Verification Model all applicants undergo a face-to-face EOI check at a Gatekeeper accredited Registration Authority (RA) in accordance with sections 3.2 through 3.4 of this CP. Also refer to Appendix E for a description of initial identity verification under additional EOI Models. The RA shall perform the identity verification specific to the Formal Identity Verification EOI model and the Certificate Type being issued. The end entity Certificate issued shall indicate the EOI model used in identity verification and application processing.

Initial verification establishes the identity of the individual Key Holders (in their capacity as Individuals or as representatives of Organisations). For the issuance of digital certificates to individual Key Holders in their capacity as representatives of Organisations, both the identity of the representative and the identity of the Organisation shall be verified and both the Key Holder and the Organisation are identified within the digital certificate itself.

With respect to establishing the identity of the Organisation, additional steps are required to establish the authority of the Certificate Manager to hold and use a Gatekeeper Manager Certificate on behalf of the Organisation. The Gatekeeper Manager Certificate issued to the Certificate Manager will itself subsequently serve as EOI of the Certificate Manager and their authority to request other digital certificates, ie, to make the request to the CA for the issuance of the Device Certificate or other Business Certificates for the Organisation.

The issuance of an Individual Certificate can subsequently be used as authentication for providing information to the CA to identify a device or application for the issuance of the Device Certificate.

3.2.1 Method to Prove Possession of Private Key

The Symantec CA 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 CA-approved method

3.2.2 Authentication of Organisation Identity

Applications can be made for digital certificates for representatives of Organisations (including Certificate Managers and Key Holders). In terms of Organisation Identity, these applicants are authenticated in terms of the identity of the Organisation as well as the binding of the person to the Organisation.

The Organisational documents presented for establishing the Organisation identity must:

- identify the Organisation;
- confirm that the named Authoriser is a member of the Organisation (via an ASIC check, ABR search and/or an out-of-band check such as phone verification); and
- indicate that the Authoriser has approved a Certificate Manager for the Organisation.

Symantec will reject an application[1] if the Organisation Applicant or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is:

(a) Identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organisation or person under the laws of the country of Symantec's jurisdiction(s) of operation; and

(b) Has its Jurisdiction of Incorporation or Registration or Place of Business in any country with which the laws of Symantec's jurisdiction prohibit doing business

Symantec takes reasonable steps to verify the Organisation applications with the following US Government Denied lists and regulations[2]:

- BIS Denied Persons List
- BIS Denied Entities List
- US Treasury Department List of Specially Designated Nationals and Blocked Persons
- US Government export regulations

The Organisation identity documentation must comprise either Option 1 OR Option 2:

Options	Organisation Identity Documentation Requirement
Option 1	– An original or certified copy of the notice issued by the Registrar of the Australian Business Register (ABR) bearing the business entity's name and the Australian Business Number (ABN). If either the owner, chief executive or other officer or employee with clear capacity to commit the business entity is named as the Public Officer on the document issued by the Registrar of the ABR, then this document only will suffice; and – A secondary check involving online verification with the ABR to link the Organisation's ABN to its business name is recommended.
Option 2	– If the notice issued by the Registrar of the ABR cannot be provided, then a legal or regulatory document Binding either the individual or the Authoriser to the business entity; and –online verification with the ABR to link the Organisation's ABN to its business name must be achieved.

Table 2: Organisation Identity Binding Options

Prior to issuance of a certificate containing an Organisation identity, the intended Key Holder's binding to the Organisation named in the Certificate shall be established by a formal letter of authorisation from an Authoriser (sighted by the RA) that the individual is authorised to apply for a digital certificate on behalf of the Organisation. If the Key Holder is an intended Certificate Manager, the RA shall perform validation of authority in accordance with section 3.2.6.

Prior to issuance of a certificate containing an Organisation identity, the intended Key Holder (Certificate Manager or Organisational representative) named in the Certificate shall undergo an individual EOI check in accordance with the Authentication of Individual Identity, section 3.2.3.

3.2.2.1 Delegated RA Process

Under a Delegated RA process the Certificate Manager shall vouch for the identity of all representatives for whom additional Business Certificates are requested. The Certificate Manager shall present a valid Gatekeeper Manager

[1] In the case of customer disputes regarding close matches, Symantec determines/verifies the accuracy of the match with steps including detailed personal identity verification and approval by the Symantec Trade Compliance Office that oversees compliance with US export control regulations.

[2] All data is transmitted and handled in accordance with the Symantec Privacy Policy.

Certificate for authentication and the Organisation information contained within the Gatekeeper Manager Certificate shall be used in the Distinguished Name of the Certificate to be issued.

The Business Certificate request processing is exempt from RA authentication of the Organisation (section 3.2.2.1) and the Individual (section 3.2.3). Because the Certificate Manager uses their Gatekeeper Manager Certificate for authentication and authorisation, it can be assumed for the purpose of this CP that the Organisation has been verified. The act of requesting an additional Certificate through a Certificate Manager shall be construed as evidence that the identity of the proposed Key Holder has been verified. Under a Delegated RA process, the CA shall confirm that the person authorizing the Issuance of a Certificate is a current Certificate Manager of the Organisation based on presentation of a valid Certificate Manager Certificate.

The Symantec RA shall perform uniqueness validation of the Certificate DN to accept the request for additional Business Certificates.

3.2.3 Authentication of Individual Identity

Applications can be made for digital certificates by both Individuals and representatives of Organisations (including Certificate Managers and Key Holders). These applicants are authenticated in terms of the binding between the physical person and their documented identity. It is important for an RA to (at a minimum) have sighted a document that bears a biometric (signature or photograph).

Representatives of Organisations are authenticated in terms of those bindings that apply to the Individual as well as the binding between the person and the Organisation as described in section 3.2.2.

The Individual shall undergo identity verification by an accredited RA in accordance with the gatekeeper EOI Policy at *www.gatekeeper.gov.au*.

3.2.4 Authentication of Device Identity

The CA shall confirm that the person requesting the issuance of a Certificate is a current Certificate Manager of the Organisation based on presentation of a valid Gatekeeper Manager Certificate. The Organisation information of the Certificate Manager shall be used in the Distinguished Name of the Device. Because the Certificate Manager uses their Gatekeeper Manager Certificate for authentication and authorisation, it can be assumed for the purpose of this CP that the Organisation has been verified.

The Certificate Manager provides the relevant digital certificate information identifying the device to the CA within the Device Certificate request. The Symantec RA shall not verify the accuracy of the device information submitted.

The Symantec RA shall perform uniqueness validation of the Certificate DN to accept the request for a Device Certificate.

3.2.5 Non-Verified Subscriber Information

The business unit within an Organisation supplied in the certificate information is not verified.

The identification (name or description) and location information of devices and applications supplied by the Certificate Manager used in the Device Common Name is not validated by the RA.

RAs are not required to investigate or ascertain the authenticity of any document received by the RA as evidence of any matter required as part of the Registration process unless they are aware, or should reasonably be aware, that the document is not authentic.

3.2.6 Validation of Authority

The individuals duly authorised in the roles of Authoriser and Certificate Manager shall be validated in accordance with the following subsections prior to acting in their respective roles. The individuals duly authorised in the role of Certificate Manager shall subsequently present their Gatekeeper Manager Certificate for authentication in online functions.

3.2.6.1 Role of Authoriser

The Symantec RA shall verify the authorisation of the person identified as Authoriser for an Organisation. Authorisation of the individual's association with the Organisation must be evidenced by reference to:

- an authoritative public register; or
- appropriate legal, or regulatory documents issued by a government Agency.

3.2.6.2 Role of Certificate Manager

Prior to issuance of a certificate containing an Organisation identity, the intended Certificate Manager's binding to the Organisation named in the Certificate shall be established by a formal letter of authorisation from an Authoriser (sighted by the Symantec RA) that the individual is authorised to apply for a digital certificate and act in the role of Certificate Manager on behalf of the Organisation.

The Symantec RA must perform the relevant checks to verify that a person is authorised to be issued a Business Certificate in accordance with section 3.2. The Certificate issued to a Certificate Manager role shall be distinguished by the EOI Assurance Type as Certificate Manager.

3.2.7 Criteria for Interoperation

Interoperability issues are addressed through the Gatekeeper Accreditation processes and adoption of the international X.509 V3 standard.

3.3 Identification and Authentication for Re-Key Requests

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. The Symantec Gatekeeper CA requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey" although may be colloquially referred to as "renewal"). Generally speaking, this operation focuses on the fact that the old Certificate is being replaced with a new Certificate and does not emphasize whether or not a new key pair is generated.

3.3.1 Identification and Authentication for Routine Re-Key

Re-key procedures ensure that the person or organisation seeking to renew/rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate. The re-key procedure shall utilise an EOI check cycle that distinguishes the type of identification and authentication permitted per cycle.

A face-to-face EOI check in accordance with section 3.2.3 serves to start or subsequently reset the EOI check cycle. Following a face-to-face EOI check, the next re-key event is considered to be the "first" re-key event. Each re-key check cycle is initiated in anticipation of the end of the certificate operational periods established in section 6.3.2.

The "first" and "second" re-key event may be facilitated online by the Key Holder using his/her valid (not revoked or expired) certificate as identity authentication for the re-key request under the following conditions:

a) the verification process specified in section 3.2.3 was successfully completed for the previous Certificate and the registration information in the DN has not subsequently changed;
b) the RA who initially instructed the Symantec CA to issue a Certificate to the Subscriber continues to operate without compromise;
c) a request for Renewal:
    - is made prior to expiry of the Subscriber's current Certificate(s); and
    - is digitally signed using the Subscriber's current Private Key or by using the current Private Key to access the Certificate Manager portal to request the renewal. For the Standard Business Certificate and Device Certificate the Certificate Manager's current Private Key is authenticated in place of the Subscriber's Private Key.

If the above conditions are not met for the "first" or "second" re-key event request or if the request is a "third" re-key event, the Subscriber, Key Holder or Certificate Manager requesting re-key/renewal must repeat the initial identity verification process as described in the following table by Certificate Type.

Certificate Type	EOI Cycle Requirements
Individual Certificate	All Key Holders shall repeat the initial identity verification process through a face-to-face EOI check with an RA in accordance with the EOI requirements in section 3.2.
Symantec Gatekeeper Manager Certificate	All Certificate Managers shall repeat the initial identity verification process through a face-to-face EOI check with an RA in accordance with the EOI requirements in section 3.2.
Standard Business and Device Certificate	Entities holding the Standard Business Certificate or Device Certificate shall conduct the Certificate Re-Key cycle through their Certificate Manager. Organisations (and their Certificate Managers) are responsible for ensuring that the identity of additional Certificate Holders is verified prior to certificate renewal in accordance with the EOI requirements in section 3.2.

Table 3: Re-Authentication EOI Requirements

3.3.2 Identification and Authentication for Re-Key After Revocation

Following revocation, the Subscriber may request a new Certificate through a Replacement Certificate process. The Replacement Certificate shall contain the same Subscriber DN and end validity period as the revoked Certificate being replaced. A new key is generated for the Replacement Certificate.

The replacement procedure ensures that the person or organisation seeking to replace an end-user Subscriber Certificate is in fact the Subscriber of the Certificate. The Replacement Request is processed under the following conditions:

a) the certificate being replaced is in Revoked status;
b) the identity of the Subscriber has been successfully validated in accordance with Table 4;
c) successful presentation of two unique secret codes transmitted to the Subscriber/Certificate Holder via two separate channels following successful identity verification. These codes serve to authenticate the Subscriber/Certificate Holder for download of their certificate.

If the above conditions are not met, the Subscriber, Key Holder or Certificate Manager requesting replacement must repeat the initial identity verification process set out in section 3.2.

The following table describes the requirements for identity verification of the Subscriber for a Replacement Certificate.

Certificate Type	Identity Verification Requirements
Individual Certificate	All Key Holders shall undergo a successful question-and-answer with an RA using verification information provided during initial enrollment as per section 4.1.2. All information shall be accurately answered for successful validation.
Business Certificate	All Certificate Managers shall undergo a successful question-and-answer with an RA using verification information provided during initial enrollment as per section 4.1.2. All information shall be accurately answered for successful validation.

Table 4: Replacement Certificate Identity Verification Requirements

3.4 Identification and Authentication for Revocation Request

Before processing a request for Revocation of a Certificate, the Symantec CA must verify that the request is made by a person or entity authorised to request Revocation of that Certificate in accordance with section 4.9.2.

3.4.1 Individual and Business Certificate

A request for Revocation can be verified in one of the following ways:

a) the request is digitally signed with the Private Key of the Subscriber;
b) the request is made in person, and the authority of the requestor is verified as required under section 3.2.6 (validation of authority);
c) the request is made using a Challenge Phrase provided by the Subscriber at the time of Registration;

d) successful question-and-answer with the Symantec RA;
e) successful login to the Certificate Manager portal (by Certificate Manager) using his/her Private Key; or
f) a written request via fax containing the certificate details and the reason for revocation. In the case of Business Certificates, the request must be on the letterhead of the organisation and must be signed by the Subscriber, Key Holder, Certificate Manager or an authorised representative of the organisation.

The Symantec CA's detailed procedures for verifying Revocation requests is set out in the CA Operations Manual.

3.4.2. Device Certificate

A request for Revocation can be verified in one of the following ways:

a) the request is digitally signed with the Private Key of a Certificate Manager;
b) the request is made in person, and the authority of the requestor is verified as required under section 3.2.6 (validation of authority) for Business certificates;
c) the request is made using a Challenge Phrase provided at the time of Registration;
d) successful question-and-answer with the RA;
e) successful login to the Certificate Manager portal (by Certificate Manager) using his/her Private Key; or
f) a written request via fax containing the certificate details and the reason for revocation. The request must be on the letterhead of the organisation and signed by the Certificate Manager of the organisation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The Symantec CA maintains a CA Operations Manual that details the operational practices of the Symantec CA in relation to its functions and obligations under this CP.

The RA maintains an RA Operations Manual that details the operational practices of the RA in relation to its functions and obligations under this CP. Such CA and RA Operations Manuals are confidential internal documents that are not made publicly available.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Individuals acting in their private capacity can submit an application request for an Individual Certificate.

Organisations can submit an application request for a Business Certificate for an individual to represent the organisation. The Certificate Manager acting on behalf of the Organisation can submit an application request for a Business Certificate for additional Key Holders representing the organisation.

Organisations can submit an application request for a Device Certificate. The Organisation requesting a Device Certificate shall identify the Certificate Manager (person) responsible for managing the Device Certificate on behalf of the Organisation. See Appendix C for additional recommendations for Organisational processes for requesting and receipt of Device Certificates.

4.1.2 Enrolment Process and Responsibilities

Applicants must complete an Application Form available from the Symantec Gatekeeper website. In the case of Business and Device Certificates the Application Form must include authorisation from the Organisation prior to being issued a certificate in the name of the organisation.

The enrollment process varies depending on the choice of RA process and Certificate Type. A Gatekeeper accredited RA performs Individual Identity authentication for persons in their capacity as a private person requesting an Individual Certificate or as representatives of Organisations requesting a Certificate Manager Certificate and notifies the Symantec RA by sending a digitally signed email.

The Symantec RA performs Organisation Identity authentication for requests for certificates containing the Organisation name within the Subscriber DN.

Individuals requesting a Symantec Gatekeeper Manager Certificate for the role of Certificate Manager shall undergo validation of authority in accordance with section 3.2.6.

Once a Certificate Manager has been appointed within an Organisation and issued a Symantec Gatekeeper Manager Certificate, the Certificate Manager may request Device Certificates for the Organisation; such requests shall be processed in accordance with section 3.2.4.

Once a Certificate Manager has been appointed within an Organisation and issued a Symantec Gatekeeper Manager Certificate, the Certificate Manager may request Business Certificates for additional representatives of the Organisation under a Delegated RA process; such requests shall be processed in accordance with section 3.2.2.1.

Upon receipt of a duly authorized request from the Gatekeeper accredited RA, the Symantec RA shall access the CA for issuance of the corresponding certificate.

Symantec provides an online enrolment process for the issuance of Certificates using the RA. See the Symantec Gatekeeper website for further information and a step by step guide for enrolling for a Certificate. The enrollment process includes the submission of question-and-answer verification data used in the Certificate replacement process.

Following the issuance of a Symantec Gatekeeper Manager Certificate to a Certificate Manager for an Organisation, requests for additional Business Certificates may be submitted by the Certificate Manager to the same Symantec CA that supplied the Symantec Gatekeeper Manager Certificate.

The Symantec Gatekeeper Manager Certificate issued to a Certificate Manager role shall establish the EOI Assurance Type as Certificate Manager. The Standard Business Certificate issued to additional Key Holders shall establish the EOI Assurance Type as Additional Key Holder.

Under the Delegated RA process, the Certificate Manager accepts responsibility for all of its Business Certificates through acceptance of a Subscriber Agreement with the Symantec Gatekeeper CA.

Also refer to Appendix E for a description of the Enrolment Process and Responsibilities for additional EOI Models.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Applicants are authenticated in accordance with section 3.2 under the applicable EOI Model.

Applicants must provide sufficient EOI information for the Certificate Type they are applying for and be verified in accordance with sections 3.2.1 through 3.2.6, Initial Identity Validation. The following table identifies the steps for each Certificate Type:

Certificate Type	EOI Processing Step	Requirement
Individual Certificate	Bind the physical person to the name of the Key Holder as evidenced by relevant EOI documentation	Face-to-face EOI check in accordance with section 3.2.3.
Business Certificate (issued to a Certificate Manager of an organisation)[1]	Bind the Organisation to a business name and, if appropriate, to an Australian Business Number (ABN)	Organisational identity validation in accordance with section 3.2.2.
	Bind the physical person to the name of the Key Holder	Face-to-face EOI check in accordance with section 3.2.3.
	Bind the Key Holder to the Organisation	Letter of authority signed by Authoriser sighted by an RA in accordance with section 3.2.2.
	Bind the Authoriser to the Organisation	ASIC check, ABR search and/or an out-of-band check such as phone verification in accordance with section 3.2.2.
Device Certificate	Bind the Key Holder to the device/application	Use of a Symantec Gatekeeper Manager Certificate by the Certificate Manager to provide the relevant information (and evidence of the authority to make the request) to the CA for the issuance of the Device Certificate in accordance with section 3.2.4.
[1] Under the Delegated RA Process issuing additional business certificates, the EOI processing steps for the Business Certificate are exempted. Instead, the RA shall confirm that the person authorizing the Issuance of the additional business certificate is a current Certificate Manager of the Organisation and presents a valid Symantec Gatekeeper Manager Certificate with the Certificate Manager EOI Assurance Type.		

Table 5: Processing Steps by Certificate Type

For enrollments through a Certificate Manager, the Organisation information of the Certificate Manager shall be used in the Distinguished Name of the Subscriber. Because the Certificate Manager uses their Symantec Gatekeeper Manager Certificate for authentication and authorisation, it can be assumed for the purpose of this CP that the Organisation has been verified.

For Business Certificate requests, the Certificate Manager vouches for the identity of the Key Holders associated with the information supplied to be used in the Subscriber Common Name. For Device Certificate Requests, the Certificate Manager vouches for the accuracy of the device information supplied to be used in the Device Common Name. The Device Certificate information shall be constructed with values that contain no personal information.

4.2.2 Approval or Rejection of Certificate Applications

The Symantec CA is not obligated to issue Certificates to any person despite receipt of an Application. An application that has not successfully provided proof of identity shall be rejected by the RA.

The Symantec CA may refuse to issue a Certificate to any person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. On the Symantec CA's refusal to issue a Certificate, the Symantec CA shall promptly refund to the Certificate Applicant any paid Certificate enrolment fee unless the Certificate Applicant submitted fraudulent or falsified information to the RA.

The Symantec CA shall provide an explanation to all Certificate applicants whose applications have been unsuccessful.

The Symantec CA shall approve or reject requests received from the Organisation's Certificate Manager.

4.2.3 Time to Process Certificate Applications

CAs and RAs begin processing certificate applications within a reasonable time of receipt and endeavours to process applications with 48 hours of receipt.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Upon approval of the certificate request, the CA generates and transmits two secrets to the Subscriber: a unique 40-character random code is emailed to the applicant using the email address provided in the application form, and a unique 6-digit code is sent via SMS to the Subscriber's mobile phone. The pair of shared secrets are used by the enrollment webpage to authenticate the Subscriber for certificate download.

A Certificate is issued following successful authentication of the Subscriber in the installation process. The CA creates a Certificate based on the information contained in the approved Certificate Application.

Once a Certificate is downloaded by the Subscriber, the Symantec CA shall have no continuing duty to monitor or investigate the continuing accuracy of the information in a Certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

After the RA approves a Subscriber enrollment request, the CA sends an approval e-mail to the Subscriber using the email address provided in the certificate enrollment application notifying the Subscriber that the certificate has been issued and is available for acceptance. Instructions for downloading and accepting the certificate are provided in the e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber is deemed to have accepted a certificate when he or she successfully downloads the certificate by following the process explained in the notification email. Upon download the status in the Repository is changed from pending to valid.

The Certificate Manager accepts the Device Keys and Certificates and ensures that they are properly installed on the identified device/application.

4.4.2 Publication of the Certificate by the CA

Certificates shall be published after issue in accordance with section 2.3.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with Symantec's Subscriber Agreement the terms of this CP and the relevant CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorised use and shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

Reliance on a certificate must be 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.

Before any act of reliance, Relying Parties shall 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 that is not prohibited or otherwise restricted by this CP. Symantec, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the *KeyUsage* field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate in accordance with section 4.9.6. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilise 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.

4.6 Certificate Renewal

Technically, Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. This is not supported for the Symantec Gatekeeper General Category PKI. See section 4.7 for Certificate Re-Key.

4.7 Certificate Re-Key

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. The Symantec Gatekeeper CA requires that the Subscriber generate a new key pair to replace the expiring key pair. Although this may be colloquially referred to as certificate "renewal", technically Symantec Gatekeeper achieves this operation through certificate "re-key".

Each re-key cycle is initiated in anticipation of the end of the certificate operational periods established in section 6.3.2. The Symantec CA shall notify the certificate holder via the email address on the certificate prior to the expiry of the certificate. The email shall contain instructions on how to re-key (renew) the digital certificate. Certificate Managers can access Gatekeeper Account Management (GAM) to check certificates up for renewal.

4.7.1 Circumstances for Certificate Re-Key

The General Category certificate has a maximum validity period of two years. Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. Should the Subscriber fail to re-key the certificate prior to the end of the certificate validity period, the certificate will expire. Expiration of a Certificate does not affect the validity of any underlying contractual obligations created under the CPS or this CP.

Renewal of a revoked Certificate is not permitted after Revocation regardless of the reason for Revocation. Following Revocation, a Subscriber may request a Replacement certificate as described in section 3.3.2.

4.7.2 Who May Request Certification of a New Public Key

The Certificate Holder may request the re-key (renewal) of his/her own Business Certificate. However, in organisations where a Certificate Manager is appointed, the Certificate Manager may request the re-key on behalf of other Certificate Holders. Individuals holding an Individual Certificate shall manage their own certificate re-key cycle.

Only a Certificate Manager will be able to request the re-key of the Device Certificate.

4.7.3 Processing Certificate Re-Key or Replacement Requests

The Re-Key request is processed to ensure that the person or organisation seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorised by the Subscriber) of the Certificate. The Certificate Holder shall either send a digitally signed email using their valid certificate or present their valid certificate via the Gatekeeper Account Management (GAM) tool. Other Business or Device Certificate renewal requests must be approved by the Certificate Manager prior to issuance by the Symantec CA.

Certificate re-key requests shall be processed as described in Section 3.3.1 to utilise the requisite identification and authentication requirements for the specific Re-Key cycle.

Requests for Certificate replacement following revocation shall be processed as described in Section 3.3.2 to utilise the requisite identification and authentication requirements.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of the issuance of a re-keyed certificate to the Subscriber is in accordance with section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting acceptance of a re-keyed certificate is in accordance with section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Publication of a re-keyed certificate is in accordance with section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the Subscriber's public key). Certificate modification is considered a new Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

See Sections 4.1 and 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The Symantec CA shall revoke a Certificate on request of a person specified in section 4.9.2.

The Symantec CA shall revoke a Certificate (whether or not it has received a request to do so) where it becomes aware of (or reasonably suspects) the following:

a) the Subscriber has ceased to belong to a specified/agreed Community of Interest;
b) the Key Holder ceases to be an employee or agent of the Organisation
c) there has been a loss, theft, modification, or other Compromise of the associated Private Key;
d) faulty or improper Registration, Key Generation or issue of a Certificate has occurred;
e) a change in the Certificate Information occurs;
f) the Key Holder's/Certificate's Private Key or Trustworthy System was Compromised in a manner materially affecting the Certificate's reliability;
g) the applicable Subscriber has not complied with an obligation under the CPS, this CP or the Subscriber Agreement;
h) another person's information has been or may be materially threatened or compromised unless the Certificate is revoked.

The Symantec CA is not required to investigate any of the circumstances for revocation, but in cases where the circumstances are investigated, they must use reasonable efforts to notify the relevant Subscriber beforehand of that intention.

Device Certificates should be revoked where any one of the following circumstances arises:

a) a Private Key is compromised;
b) media holding a Private Key is compromised or lost;
c) the Key Holder (in this instance is the device/application) ceases to exist;
d) there has been improper or faulty issuance of the Device Keys and Certificates;
e) the Certificate information becomes inaccurate;
f) a change in the Registration Information occurs;
g) the relevant CA ceases to operate;
h) the Organisation ceases to exist; or
i) the CA receives a revocation request from an Authoriser or a Certificate Manager.

4.9.2 Who Can Request Revocation

A Subscriber, or an authorised representative of a Subscriber, may request the Symantec CA to revoke his or her Certificate(s) at any time.

Revocation of a Device Certificate may be initiated by:

a) the Certificate Manager,
b) the Authoriser, or
c) the CA if it believes circumstances for revocation exist.

A PKI Entity must immediately notify the Symantec CA if:

a) it receives a request for Revocation of a Certificate(s); or
b) it becomes aware of circumstances which may justify Revocation of a Certificate(s), such as those set out in section 4.9.1.

4.9.3 Procedure for Revocation Request

A revocation request may be submitted in person, on-line webpage or sent to the Symantec RA by any of the methods identified in section 9.11 for sending requests to the Symantec GK PKI. A revocation request, which is made in person, must be made to the Symantec RA at the address set out on the Symantec Gatekeeper Website.

A request received from entities set out in section 4.9.2 is authenticated in accordance with section 3.4.

A request (including an order or direction) from any entity other than those set out in section 4.9.2, will be processed only if the Symantec CA is satisfied that the entity is lawfully empowered to request Revocation of the Certificate.

Upon revocation of a Certificate the Symantec CA must promptly notify the Subscriber that its Certificate has been revoked and update the CRL. Upon revocation of a Certificate the Certificate's Operational Period ends/expires.

The Symantec CA shall issue a notice to the Subscriber confirming the revocation of the Keys and Certificate and the date and time that the Certificate is revoked. The list of revoked Certificates is made accessible to potential Relying Parties through either LDAP or OCSP.

4.9.4 Revocation Request Grace Period

There is no revocation grace period.

4.9.5 Time within Which CA Must Process the Revocation Request

Symantec processes revocation requests within 24 hours.

4.9.6 Revocation Checking Requirement for Relying Parties

Certificate revocation checking shall be performed by the Relying Party to include the following:

a) Establishing a Certificate chain for the Certificate used to sign the information
   – in the case of a Public Hierarchy this involves confirming that the CA who issued the Certificate is a Subordinate CA of the SGR.
   – in the case of a Private Hierarchy it involves confirming that the CA who issued the Certificate is trusted by the Relying Party;
b) Checking the Repository for revocation of Certificates in this chain
   – the Relying Party must determine if any of the Certificates along the chain from the Signer to an acceptable root within the Symantec Gatekeeper PKI have been revoked by querying the CRL or OCSP responder (if available) for each certificate in the chain. A Revocation has the effect of prematurely terminating the Operational Period during which verifiable Digital Signatures can be created.

4.9.7 CRL Issuance Frequency (If Applicable)

The Symantec CA will update the CRL for end-user Subscriber Certificates at least daily. CRLs for CAs that only issue CA Certificates shall be issued at least quarterly, and also whenever a CA Certificate is revoked. CRLs shall also be issued on an emergency basis, as determined by the Symantec CA.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the Symantec Repository automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. A web-based repository permits Relying Parties to make online inquiries regarding revocation and other Certificate status information.

The appropriate URL of the OCSP responder (if any) to determine the validity of a Certificate in real time can be determined from information appearing in the Certificate.

4.9.10 On-line Revocation Checking Requirements

Prior to placing reliance upon a certificate, a Relying Party must check the status of the certificate in accordance with section 9.6.4.1. To use an OCSP responder that is provided by the Symantec CA, a person must be using appropriate software to interrogate and interpret the information provided by the OCSP responder.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

The Symantec CA shall use commercially reasonable efforts to notify potential Relying Parties if the Symantec CA discovers, or has reason to believe, that there has been Compromise of the Private Key of a Symantec CA.

4.9.13 Circumstances for Suspension

Certificate Suspension is not currently supported for Certificates.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

In the revocation of Certificates, the Symantec CA shall provide access to digital certificate status information via an approved X.509 compliant protocol (e.g. DAP, LDAP or OCSP). CAs are not confined to using a single protocol for the distribution of Certificate information. The CA shall ensure that information in Directories is synchronised.

4.10.1 Operational Characteristics

The status of public certificates is available via CRL through the Symantec Gatekeeper website (at a URL specified in the CPS), an LDAP directory and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services shall be available 24 X 7 excepting scheduled interruption.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A subscriber may end a subscription for a Symantec Gatekeeper Certificate by:

- Allowing the certificate to expire without renewing or re-keying that certificate
- Requesting revocation of the certificate before certificate expiration without replacing the certificate.

4.12 Key Escrow and Recovery

The Symantec Gatekeeper CA does not support Key Escrow.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

Symantec shall conform to the standards and guidelines stipulated by the Defence Signals Directorate Information Security Manual (ISM) where applicable.

5.1 Physical Controls

Symantec implements physical controls and security to ensure that the Symantec CA and RA are able to provide their services in a secure, reliable and trusted manner.

5.1.1 Site Location and Construction

All Symantec Gateway CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of sensitive information and systems.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or gate that provides mandatory access control for individuals and requires a positive response (e.g., door or gate unlocks or opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorised access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.

Additional detail describing the site location and construction housing the CAs and RAs is provided in the CPS.

5.1.2 Physical Access

Access to each tier of physical security shall be auditable and controlled so that each tier can be accessed only by authorised personnel. Sensitive materials, including CA cryptographic hardware and associated key material when not in use, are securely stored within storage containers with a security strength commensurate with the sensitivity of the materials being stored. Access shall be auditable and controlled to ensure access by only authorised and Trusted personnel in accordance with section 5.2.2.

5.1.3 Power and Air Conditioning

The secure facilities of CAs and RAs shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water.

5.1.5 Fire Prevention and Protection

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

CAs and RAs shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorised use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

CAs and RAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorised use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-Site Backup

CAs and RAs shall maintain back-ups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be "Trusted Persons" serving in a "Trusted Position." Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the background screening requirements of this CP.

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect the processing, 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,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of Persons Required Per Task

CAs and RAs shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place 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.

5.2.3 Identification and Authentication for Each Role

CAs and RAs shall confirm the identity and authorisation of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on Information Systems and CA or RA systems.

Authentication of identity shall include the personal (physical) presence of such personnel in front of Trusted Persons performing HR or security functions, and a check of well-recognised forms of identification, such as passports and driver's licenses. Identity shall be further confirmed through background checking procedures specified in this CP.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

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

- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

CAs and RAs shall require that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

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, and
- search of driver's license records.

Further mode, for personnel with direct physical or logical access to cryptographic materials, CA database or other resources specifically identified in the Security Risk Management Plan, Background checks in accordance with the Negative Vetting Level 1 (NegVet1) standard are conducted through the Australian Government Security Vetting Agency (AGSVA).

Background checks are repeated for personnel holding Trusted Positions at least every five (5) years.

These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity utilise 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 (but are not limited to) the following:

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

Reports containing such information are evaluated by human resources and security personnel, and such personnel take actions that are reasonable 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 are subject to applicable law.

5.3.3 Training Requirements

Symantec Gatekeeper CAs and RAs shall provide their personnel with the requisite training needed for their personnel to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel. Such training programs shall address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of the Symantec Gatekeeper PKI,
- Hardware and software versions in use,
- All duties the person is expected to perform,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Symantec Gatekeeper CAs and RAs shall provide refresher training and updates to their 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.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

CAs and RAs shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorised actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorised actions.

5.3.7 Independent Contractor Requirements

CAs and RAs may permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

- the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and
- the contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to the Symantec secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

Symantec shall provide their personnel (including Trusted Persons) with the requisite training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

The Symantec CA is required to log particular information. Details are set out in section 5.4 of the CPS.

5.4.1 Types of Events Recorded

All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. The types of auditable events logged by the CA include:

- Operational events (including but not limited to (1) the generation of a CA's own keys and the keys of subordinate CAs, (2) start-up and shutdown of systems and applications, (3) changes to CA details or keys, (4) cryptographic module lifecycle management-related events (*e.g.*, receipt, use, de-installation, and retirement), (5) possession of activation data for CA private key operations, physical access logs, (6) system configuration changes and maintenance, (7) Records of the destruction of media containing key material, activation data, or personal Subscriber information)
- Certificate lifecycle events (including but not limited to initial issuance, re-key, renew, revocation, suspension)
- Trusted employee events (including but not limited to (1) logon and logoff attempts, (2) attempts to create, remove, set passwords or change the system privileges of the privileged users, (3) personnel changes)
- Discrepancy and compromise reports (including but not limited to unauthorised system and network logon attempts)
- Changes to Certificate creation policies e.g., validity period.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed in response to alerts based on irregularities and incidents within their CA/RA systems. Audit logs are continuously processed by centralised logging. Audit log reviews shall include a verification that the log has not been tampered with and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorised viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 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, organisation, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

5.5 Records Archival

In terms of the archival of records, the Symantec CA shall comply with the *Archives Act 1983* (Cth).

Notwithstanding the sub-sections below, archival of Certificate information may be subject to jurisdictional legislation and other legal constraints which may override the conditions described.

5.5.1 Types of Records Archived

Symantec Gatekeeper RAs and CAs archive:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

The Symantec CA is required to archive particular information. Details are set out in section 5.5 of the CPS.

5.5.2 Retention Period for Archive

Audit trail information shall be kept for a minimum period of seven (7) years from the date of generation, unless the Organisation specifically requires a longer period.

5.5.3 Protection of Archive

The archive of records shall be accessible by only authorised Trusted Persons. The archive is protected against unauthorised viewing, modification, deletion, or other tampering by storage within a Trustworthy System. Archive media shall be protected either by physical security or a combination of physical security and cryptographic protection. It shall also be protected from environmental factors such as temperature, humidity, and magnetism.

The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP.

5.5.4 Archive Backup Procedures

The Symantec CA shall incrementally back-up electronic system archives on a daily basis and perform full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal vs. External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorised Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

Two years before the expiry of a Subordinate Issuing CA's Certificate, the SGR will re-certify the CA's Certificate, giving it a further 10 year Operational Period in accordance with section 6.3.2.

A CA Certificate may be re-certified if the CA's Superior Entity reconfirms the identity of the CA. Based on the results of the identity verification, the Superior Entity shall either approve or reject the renewal application. If approved, the Superior Entity shall conduct a Key Generation Ceremony in order to generate a new key pair for the CA. During such Key Generation Ceremony, the Superior Entity shall sign and issue the CA a new Certificate. New CA Certificates containing the new CA public keys generated during such Key Generation Ceremony shall be made available to Relying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of CA information including, Certificate application data, audit data, and database records for all Certificates issued, shall be kept in off-site storage and made available in the event of a compromise or disaster. The Symantec CA maintains a Disaster Recovery (DR) and Business Continuity Plan (BCP) covering all reasonably foreseeable types of disasters and compromises affecting the services under this CP including:

a) loss or corruption (including suspected corruption) of computing resources, software, and/or data of the Symantec CA or another PKI Service Provider; and
b) Compromise of the Symantec CA's Private Keys which Relying Parties rely on to establish trust in Certificates.

The Disaster Recovery and Business Continuity Plan are consistent with the requirements of the Symantec CA's Protective Security Plan. For security reasons these plans are not publicly available.

5.7.2 Computing Resources, Software and/or Data are Corrupted

Following corruption of computing resources, software, and/or data, a report of the incident and a response to the event, shall be promptly made by the affected CA or RA in accordance with Symantec's documented incident and compromise reporting and handling procedures in the applicable CPS and security policies.

If computing resources, software and/or data are corrupted, the processes outlined in the Disaster Recovery and Business Continuity Plan will be performed.

5.7.3 Entity Private Key Compromise Procedures

If a Private Key of the Symantec CA is compromised, the SGR will revoke the CA's Certificate, and report the compromise in the CRL and in the Repository.

5.7.4 Business Continuity Capabilities After a Disaster

Symantec operating secure facilities for CA and RA operations develop, maintain, annually test and, when necessary, implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions. Disaster recovery sites have the equivalent physical security protections specified by this CP.

Symantec has the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate issuance, Certificate revocation and publication of revocation information.

The Disaster Recovery and Business Continuity Plan sets out response and recovery procedures for each type of disaster or compromise.

5.8 CA or RA Termination

This section applies in the event that the Symantec CA or another PKI Service Provider intends to cease providing services, which are necessary for the issue of Keys and Certificates, or for reliance on Digital Signatures or Certificates under this CP.

The Symantec CA will give as much notice as possible of the relevant circumstances, and the actions the Symantec CA proposes for the benefit of the AGIMO, all Subscribers; and the Relying Parties of which the Symantec CA is aware.

If a PKI Service Provider (including the Symantec CA itself) unexpectedly ceases providing services the Symantec CA must immediately give notice to the affected parties to provide them the opportunity to address any business impacting issues. In the event that the Subordinate CA ceases operations, all certificates issued by the CA shall be revoked prior to the date that the Subordinate CA ceases operations. The obligations for termination under this section are in addition to any obligations the Symantec CA or any other entity has under the requirements set forth in section 5.7 (Compromise and Disaster Recovery).

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key Pair generation must be performed by the Subscriber using Trustworthy Systems and processes that provide the required Cryptographic strength of the generated Keys, and prevent the loss, disclosure, modification, or unauthorised use of such Keys.

The Symantec Gatekeeper CA shall not generate Subscriber Private Keys. A Subscriber's Key Pair(s) are generated and stored by the application that generates those Keys (eg a browser) during the Application process.

CA keys are generated in a Key Generation Ceremony. All Key Generation Ceremonies are conducted in accordance with Symantec Gatekeeper confidential security policies.

6.1.2 Private Key Delivery to Subscriber

As the Subscriber's Private Keys are generated and stored by the Subscriber's application (eg a browser), there is no need for the Symantec CA or the RA to see or deliver any Private Keys to Subscribers.

In the issuance of Device Certificates, the Private Keys are generated and stored by the Device (eg a browser or Hardware Security Module device) used by the Organisation and there is no need for the Symantec CA or the RA to see or deliver any Private Keys to Subscribers. The Organisation may be required to export the Key Pair and associated Certificate, from the browser where the Key Pair was generated, and import it into the required Device to identify the relevant application, Device, process or service for which it was issued.

6.1.3 Public Key Delivery to Certificate issuer

A Subscriber's Public Key is forwarded to the Symantec CA as part of the Key Generation process. When a Public Key is transferred to the Symantec CA to be certified, it shall be delivered through a mechanism ensuring that the Public Key has not been altered during transit and that the Subscriber possesses the Private Key corresponding to the transferred Public Key such as a PKCS#10 message or other cryptographically equivalent method.

Upon the Subscriber's acceptance of the Certificate, the Symantec CA shall publish a copy of the Certificate in the Certificate Directory and in other appropriate locations, as determined by the Symantec CA.

6.1.4 CA Public Key Delivery to Relying Parties

The Symantec CA's Public Key is delivered to the Key Holder as Relying Party as part of the process of issuance of a Certificate to a Subscriber in an online transfer meeting the IETF RFC 2510 (PKI Certificate Management Protocols) standard using Evaluated Products, or equally secure non-electronic means.

The Public Keys of all Subordinate CAs, will be made available for download via the Repository.

6.1.5 Key Sizes

The Symantec Issuing CA's online Application process checks the key size of keys and ensures that all keys generated by the applicant are 2048 bits or longer.

Key Pairs are generated by the Subscriber using algorithms embedded in the application/hardware used to generate the Keys. These algorithms should be of the strength and type specified on the Evaluated Products List.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per x509v3 field)

Key usage is defined in accordance with RFC 5280 for X.509 version 3 certificates. Under the General Category Individual and Business certificate types, single-use certificates shall be issued as follows:

- Encryption Certificate with Key Usage set to *KeyEncipherment* and *DataEncipherment*.
- Signing Certificate with Key Usage set to *DigitalSignature*.

Under the General Category Device certificate type, dual-use Device Certificates shall be issued with Key Usage set to *DigitalSignature, KeyEncipherment* and *DataEncipherment*.

Additional information on key usage is provided in the Certificate Profile in section 7.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

Subscribers should instigate their own policies to ensure the integrity, and security of their Private Keys. Private Keys shall be protected by Subscribers using a Trustworthy System and Subscribers shall take necessary precautions to prevent the loss, disclosure, modification or unauthorised use of such Private Keys.

Symantec CA private keys are subject to multi-person control over activation of or access to the hardware cryptographic device containing the private key in accordance with sections 5.2.2 and 5.2.3.

6.2.1 Cryptographic Module Standards and Controls

Private keys within the Symantec Gatekeeper PKI shall be protected using a Trustworthy System.

The Symantec Gatekeeper CAs shall perform all CA cryptographic operations on cryptographic modules which are EAL4+ evaluated. All RA cryptographic operations shall be performed on a cryptographic module rated at FIPS 140-1 level 2.

The Subscriber should ensure that the Cryptographic Module used to store its Private Key adequately protects its Private Key from Compromise in accordance with Subscriber Obligations, section 9.6.3.

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

Both the operational and backup versions of Symantec CA private keys are subject to multi-person control over activation of or access to the hardware cryptographic device containing the private key in accordance with sections 5.2.2 and 5.2.3.

Symantec utilises Secret Sharing (multi-person control) to protect the activation data needed to activate the CA private keys in accordance with the Symantec Gatekeeper confidential security policies. CAs use “Secret Sharing” to split the private key or activation data needed to operate the private key into separate parts called “Secret Shares” held by individuals called “Shareholders.” Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) shall be required to operate the private key. Symantec enforces a threshold of three (3) shares to sign a CA certificate.

For disaster recovery tokens, the threshold number or required shares remains the same while the number of shares distributed may be less than the number distributed for operational tokens.

6.2.3 Private Key Escrow

The Symantec CA shall not provide Key Escrow.

6.2.4 Private Key Backup

Symantec shall back up the CA private keys to enable recovery from disasters and equipment malfunction in accordance with Symantec Gatekeeper confidential security policies. Back-ups shall be made by copying CA private keys and entering them onto back-up cryptographic modules in accordance with Section 6.2.6 and 6.2.7.

Private keys that are backed up shall be protected from unauthorised modification or disclosure through physical or cryptographic means. Back ups are protected with a level of physical and cryptographic protection equal to or

exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe.

Subscribers may make their own arrangement for backup of their Private Keys used for decryption. Backup of keys with Key Usage set to *Digital Signature* is discouraged.

The Symantec CA recommends the Organisation back up Device Certificates for business continuity purposes. For purposes other than business continuity, only keys with the Key Usage set to *Encipherment* should be backed up and archived.

6.2.5 Private Key Archival

Upon expiration of a CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least five (5) years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CPS.

Subscribers and Organisations may make their own arrangement for archival of historical Private Keys used for encryption. Upon expiration the Private Keys used for Signing are no longer used and archiving is not required.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private key.

The generation of CA or RA private keys on one hardware cryptographic module and transferring them into another shall be performed securely to the extent necessary to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens in accordance with Symantec Gatekeeper confidential security policies. Private keys shall be encrypted during such transfer.

The Subscriber should ensure that their Private Keys are entered into a Cryptographic Module (eg, software key store) in an appropriate manner to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

Activation of the CA private key is performed by authorised Trusted Persons under multi-person control in accordance with section 6.2.2.

For private key protection, Symantec RAs shall use a cryptographic module that requires them to:

- Present the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the RA 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 RA's authorisation.

It is strongly recommended that the Subscriber or Key Holder (including Certificate Managers serving in the role of delegated RA) restrict access to the Private Key by use of Activation Data, so that before an operation requiring the Private Key may be commenced the Activation Data known only to the Key Holder must be entered. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged. Subscribers have the option of using enhanced Private Key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

6.2.9 Method of Deactivating Private Key

When an online CA is taken offline, the CA personnel shall remove the token containing such CA's private key from the Reader in order to deactivate it.

RAs have an obligation to protect their private keys after a private key operation has taken place. The private key may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card Reader.

The Subscriber should ensure that their Private Keys are deactivated after usage in an appropriate manner to prevent unauthorised use of such private keys.

6.2.10 Method of Destroying Private Key

When required, CA and RA private keys are destroyed in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key in accordance with the Defence Signals Directorate Information Security Manual (ISM). Such a process shall be witnessed in accordance with Symantec Gatekeeper confidential security policies.

Subscriber Private Keys should be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure, or unauthorised use.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CAs shall archive their own public keys. No stipulation for Subscribers.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The SGR CA shall certify or re-certify the Symantec Subordinate CA's Certificate, giving it a 10 year Operational Period. A CA shall not issue Certificates with Operational Periods that extend beyond the usage period of the key pair of the Subordinate CA itself. Therefore, the CA key pair usage period is necessarily shorter than the operational period of the CA Certificate and the Symantec CA shall be re-certified two years prior to the expiry of the CA certificate (specifically, the length of the Operational Period of the end entity Certificates that the CA issues).

Upon the end of the Operational Period for a CA key pair, the CA shall thereafter cease all use of the key pair, except to the extent a CA needs to sign revocation information until the end of the Operational Period of the last Certificate it has issued.

The Operational Period for end-user Subscriber key pairs is the same as the Operational Period for their Certificates, except that keys may continue to be used after the Operational Period for data decryption and signature verification. The Operational Period of a Certificate ends upon either its expiration or revocation. Subscribers shall cease all use of their Authentication (Signing) Private Key at the end of the Operational Period.

The Operational Period for Subscriber Certificates shall be set according to the time limits set forth in the following table.

Certificate Type:	***Validity Period***
Individual Encryption and Individual Signing Certificates	Up to two years.
Business Encryption and Business Signing Certificates	Up to two years.
Device Certificate	Up to two years.

Table 6: Certificate Validity Periods

6.4 Activation Data

Activation Data refers to data other than the keys that are required to operate Cryptographic Modules (eg password and pins).

6.4.1 Activation Data Generation and Installation

The Symantec CA generates activation data for their CAs' private keys and RAs, in accordance with the Secret Sharing requirements of this CP and the Symantec Gatekeeper confidential security policies. The Symantec CA generates a pair of unique, random installation codes transmitted to the Subscriber for authentication for download of the certificate.

Installation codes are generated by Symantec for authentication of the Subscriber for download of the certificate at issuance. Subscribers shall also generate and use Activation Data for their Private Keys so as to protect against the loss, theft, modification, unauthorised disclosure, or unauthorised use of the Private Keys. To the extent passwords are used as activation data, Subscribers shall generate passwords that cannot easily be guessed or cracked by dictionary attacks.

6.4.2 Activation Data Protection

The Symantec CA utilises Secret Sharing in accordance with this CP and the Symantec Gatekeeper confidential security policies. Such security policies provide Shareholders with the necessary secure procedures and precautions to prevent the loss, theft, modification, unauthorised disclosure, or unauthorised use of the Secret Shares that they possess.

The installation codes generated by Symantec for authentication of the Subscriber for download of the certificate are single use codes and transmitted to the Subscriber by separate channels. Subscribers shall also protect Activation Data of their Private Keys in accordance with section 6.4.1.

6.5 Computer Security Controls

CA and RA functions take place on Trustworthy Systems in accordance with the Symantec Gatekeeper confidential security policies.

6.5.1 Specific Computer Security Technical Requirements

Symantec shall ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorised access. In addition, CAs limit access to production servers to those individuals with a valid business reason for access. General application users shall not have accounts on the production servers.

The CA shall have production networks logically separated from other components to prevent network access except through defined and authorised application processes.

RAs shall ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorised access. RAs shall logically separate access to these systems and this information from other components to prevent access except through defined and authorised processes.

Direct access to sensitive systems and repositories shall be limited to Trusted Persons in Symantec's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

Symantec Gatekeeper shall use computer systems with security ratings as specified within the Protective Security Plan (PSP).

6.6 Life Cycle Technical Controls

Details of the Symantec CA's life cycle technical controls can be found in the CA Operations Manual.

6.6.1 System Development Controls

Symantec Gatekeeper shall adopt system development controls as specified within the Protective Security Plan (PSP).

6.6.2 Security Management Controls

Symantec Gatekeeper shall adopt security management controls as specified within the Protective Security Plan (PSP).

6.6.3 Life Cycle Security Controls

Symantec Gatekeeper shall adopt lifecycle security controls as specified within the Protective Security Plan (PSP).

6.7 Network Security Controls

CA and RA functions are performed using networks secured in accordance with Symantec Gatekeeper confidential security policies to prevent unauthorised access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 End Entity Certificates

Refer to the Symantec Gatekeeper General Category CPS for detailed Certificate Profiles.

7.1.2 Version Number(s)

The Symantec Gatekeeper Certificates shall be X.509 Version 3 Certificates.

7.1.3 Certificate Extensions

The Symantec CA shall populate X.509 Version 3 Certificates with the extensions indicated in the Certificate Profiles, section 7.1.1 of the CPS.

7.1.4 Algorithm Object Identifiers

See this section in the CPS.

7.1.5 Name Forms

Certificates issued under this CP must contain the full Distinguished Name of the CA Issuing the Certificate in the "Issuer" field, and the Subscriber (and the Organisation) in the "Subject" field in accordance with the Certificate Profiles, section 7.1.1.

7.1.6 Name Constraints

No stipulation.

7.1.7 Certificate Policy Object Identifier

The Symantec CA supports the use of the Certificate Policy Object Identifier as is indicated in the Certificate Profile.

7.1.8 Usage of Policy Constraints Extension

Certificates issued under this CP contain 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 applicable CPS.

7.1.9 Policy Qualifiers Syntax and Semantics

See this section in the CPS.

7.1.10 Processing Semantics for the Critical Certificate Policies Extension

The Certificate Policies extension is not critical.

7.2 CRL Profile

7.2.1 Version Number(s)

The CRLs issued under this CP will be X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

7.3.1 Version Number(s)

Symantec supports Version 1 of the OCSP specification defined by RFC2560 and Version 1 of the OCSP specification defined by RFC 5019.

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The Symantec CA and RA is required to conduct periodic audits of its operations. Additionally, in accordance with Gatekeeper requirements, the Symantec PKI must undergo an annual compliance audit by a member of the Audit Panel listed on the Gatekeeper website.

8.2 Identity/Qualifications of Assessor

Gatekeeper auditors are approved by the Competent Authority on the basis of expertise in relation to Digital Signature technology, information technology security procedures or any other relevant areas of expertise required of an auditor to enable evaluation to be carried out properly and expertly against the Gatekeeper CA and RA Accreditation Criteria.

8.3 Assessor's Relationship to Assessed Entity

Gatekeeper auditors will be independent of the audited entity.

8.4 Topics Covered by Assessment

The purpose of Gatekeeper audits is to ensure that the Symantec CA and RA:

(a) maintains compliance with Gatekeeper Accreditation criteria and policies; and
(b) continues to operate as required by the Approved Documents.

8.5 Actions Taken as a Result of Deficiency

Actions recommended by the auditor arising from any deficiency revealed by a Gatekeeper audit will be discussed by the audited entity and authorised representatives of Finance. If necessary, the Competent Authority may direct the audited entity to take certain remedial action. Failure to adequately address deficiencies identified in an audit may result in withdrawal of the entity's Gatekeeper Accreditation.

8.6 Communication of Results

The date on which the Symantec Gatekeeper CA or RA was last audited will be published on the Symantec Gatekeeper Website and may also be published by Finance.

The results of a Symantec Gatekeeper audit are confidential and will be communicated by the auditor only to authorised representatives of Finance and the audited entity. Results of the compliance audit of the Symantec Gatekeeper CA and RA operations may be released at the discretion of Symantec Gatekeeper management.

9. OTHER BUSINESS AND LEGAL MATTERS

This CP serves as notice of the rules governing the respective rights and obligations of the PKI Entities among themselves.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The Symantec CA fees charged for Certificates and related services can be obtained from the Symantec Gatekeeper Website.

9.1.2 Certificate Access Fees

Certificates are published in the Certificate Directory. There is no additional fee for accessing Certificates.

9.1.3 Revocation or Status Information Access Fees

Revocation status is published in the CRL. There is no additional fee for accessing the CRL.

9.1.4 Fees for Other Services

Fees for other Symantec services can be obtained from the Symantec Gatekeeper Website.

9.1.5 Refund Policy

There is a charge per Certificate issued. Refunds for certificates issued erroneously will not be given as a matter of course except where Symantec is responsible for the error. Symantec may in its discretion issue a refund for a certificate, or issue a replacement certificate free of charge.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Symantec shall 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.

9.2.2 Other Assets

Symantec Australia Pty Ltd is listed on the Multi use list maintained by Finance at *https://www.tenders.gov.au/?event=public.MUL.list*.

9.2.3 Insurance or Warranty Coverage for End-Entities

Symantec does not provide any insurance and/or extended warranty coverage for end-entity certificates issued pursuant to the Gatekeeper 2.0 framework.

9.3 Confidentiality of Business Information

Each PKI Entity must protect Confidential Information it holds in accordance with Symantec's security policy documented in its security profile.

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by RAs and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Symantec Gatekeeper audit trail records,
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of Symantec Gatekeeper hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Data supplied by Subscribers and placed within the Certificate become public by its nature and therefore shall not be considered Confidential Information. Certificates, Certificate revocation and other status information, repositories of the Symantec Gatekeeper PKI, and information contained within them are not considered Confidential/Private Information. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Symantec Gatekeeper participants receiving confidential information shall secure it from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

Each PKI Entity must protect Private Information it holds against unauthorised disclosure.

9.4.1 Privacy Plan

Registration information may contain personal information about Key Holders. The RA must not collect any personal information about Key Holders as part of the Registration process other than the registration information and other necessary information to complete the transaction.

The Symantec CA and the RA must comply with their obligations under the *Privacy Act 1988*, including (where applicable) the Australian Privacy Principles (APPs) as established by the Privacy Amendment Bill 2012.

When providing services to or in relation to a Commonwealth Agency, the Symantec CA and the RA must also comply with the Information Privacy Principles, as if they were Agencies of the Commonwealth of Australia.

When providing services to or in relation to a State or Territory Agency, the Symantec CA and the RA must also comply with:

a) any privacy law applicable to service providers to that agency; and
b) any other privacy obligations imposed by or in relation to that agency.

The subject of any personal information held by a PKI Service Provider shall on request be provided with that information in accordance with the PKI Service Provider's personal information access protocol, and the privacy obligations applicable to the PKI Service Provider under this CP, and if there is any inconsistency between the two, in accordance with those privacy obligations.

9.4.2 Information Treated as Private

Personal information collected as part of the Registration process transaction that is not contained within the Certificate or the CRL is treated as Private.

9.4.3 Information Not Deemed Private

Personal information contained within the certificate is not deemed private. Subscribers agree to the publication, through the Certificate Directory and CRL, of any personal information which forms part of the Certificate information.

Revocation of a Certificate published in the CRL in accordance with this CP is also not deemed private.

9.4.4 Responsibility to Protect Private Information

Certain information that is deemed private and provided to a PKI Service Provider will be protected under specific legislation, or guidelines. The PKI Service Provider agrees to protect that information in accordance with the applicable legislation or guidelines, or in accordance with any procedures agreed between the PKI Service Provider and an Agency.

9.4.5 Notice and Consent to Use Private Information

Subject to any applicable law or legal restriction, Personal Information held by a PKI Entity about a Subscriber may be disclosed to a third party where the Subscriber has authorised the disclosure in writing.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Personal Information, Confidential Information and other information which is protected under sections 9.4.2 and 9.4.4 must not be released by a PKI Service Provider except under a properly constituted order from a court or other body having power to require production of that information, or unless otherwise legally required or authorised.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Unless otherwise agreed between the relevant PKI Entities:

a) Intellectual Property Rights (IP Rights) in the Approved Documents, the Certificate Directory and the CRL are owned by Symantec;
b) IP Rights in Certificates are owned by Symantec, subject to any pre-existing IP rights which may exist in the Certificates or the Certificate Information; and
c) any IP rights in Key Pairs are owned by the PKI Entity which generated the Key Pair.

Subject to the first paragraph of this Section 9.5 and unless otherwise agreed, Symantec grants to PKI Entities a revocable, nonexclusive, non-transferable licence to view, display and use the Approved Documents, the Certificate Directory, the CRL and Certificates as reasonably required by the PKI Entity to perform its roles and functions as a participant in Symantec's Gatekeeper PKI, subject to and as described by this CP and the CPS.

9.6 Representations and Warranties

This section sets out important obligations and responsibilities of PKI Entities operating under this CP and the corresponding CPS.

End Entities and any non-Symantec PKI Service Provider agree not to monitor, interfere with, or reverse engineer the technical implementation of the services provided by the Symantec CA or the RA except as explicitly permitted by this CP or upon prior written approval from Symantec.

9.6.1 CA Representations and Warranties

The Symantec Issuing CAs must meet all the CA obligations set out in this section for the Symantec CA. The CA warranties regarding the performance of RA duties external to Symantec are supported by agreements established with the external RA.

The Symantec CA which is Issuing a Certificate to the Subscriber, will ensure that:

a) the RA has confirmed that verification has been successfully completed in accordance with sections 3.2 through 3.4;
b) the RA attests to have accurately transcribed the Certificate Information provided by the Authoriser or Certificate Manager into the Certificate;
c) all material information contained in the Certificate (other than that specified in paragraph (b)) is accurate; and
d) the Certificate contains all the elements required by the Certificate Profile.

The Symantec CA neither generates nor holds the Private Keys of Subscribers. The Symantec CA cannot ascertain or enforce any particular Private Key protection requirements of any Organisation or Subscriber as recommended in section 6.

The Symantec CA will:
a) ensure the availability of a Certificate Directory and CRL in accordance with section 4.10;
b) promptly revoke a Certificate if requested by the Subscriber or as otherwise required in accordance with section 4.9; and
c) ensure that the date and time when a Certificate is issued or revoked can be determined precisely.

The Symantec CA will:
a) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the provision of the certification services, and in particular, personnel who possess competence at managerial level, expertise in Digital Signature technology and familiarity with proper security procedures;
b) apply administrative and management procedures which are appropriate for the activities being carried out;
c) use Trustworthy Systems and Evaluated Products which are protected against modification, and ensure the technical and Cryptographic security of the process supported by them; and
d) ensure that all relevant information concerning a Certificate is recorded (electronically or otherwise) for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

9.6.2 RA Representations and Warranties

The RA must:
a) properly conduct the verification process in accordance with sections 3.2 through 3.4;
b) ensure the accuracy and completeness of any part of the Certificate Information which is generated or compiled by the RA;
c) ensure that all relevant information concerning a Certificate is recorded (electronically or otherwise) for an appropriate period of time (in the case of Certificates being issued to an Agency, as specified in policies and guidelines issued by the National Archives of Australia under the Archives Act 1983 (Cth)), and in particular, for the purpose of providing evidence for the purposes of legal proceedings;
d) utilise Trustworthy Systems, procedures and human resources in performing its services; and
e) comply with any other relevant provisions of this CP (in particular, sections 9.3 and 9.4) and the Approved Documents.

9.6.3 Subscriber Representations and Warranties

The Subscriber representations and warranties pertain to all Subscribers of the Symantec Gatekeeper CA regardless of the EOI Model.

Where an entity accepts Keys and Certificates issued under this CP, that entity is deemed to be bound by the provisions of this CP applicable to:
a) the applicant – when it submits an application for a Certificate; and
b) the Subscriber and/or Key Holder – when it accepts the Subscriber Agreement itself or on behalf of the entity.

An applicant becomes a Subscriber (for Individual Certificates) or a Key Holder (for Business Certificates) when a Certificate is issued to and accepted by them. In the case of the Business Certificate, the obligations of a Subscriber are shared between the Organisation and the individual Key Holder who acts on behalf of the Organisation as set out in this section. In the case of the Device Certificate, the obligations of a Subscriber are shared between the Organisation and the Authoriser who acts on behalf of the organisation as set out in this section.

Each applicant must securely generate his, her, or its own Private Key(s), using a Trustworthy System, and take necessary precautions to prevent their Compromise, loss, disclosure, modification, or unauthorised use. Applicants must comply with section 6 of this CP.

Each Certificate applicant, Subscriber and Subscriber Organisation acknowledges that they and not Symantec are exclusively responsible for protecting their private key(s) from compromise, loss, disclosure, modification or unauthorised use.

The Subscriber must notify the Symantec CA of any inaccuracy or defect in the information in a Certificate promptly after receipt of the Certificate or publication of the Certificate in the Repository, or upon earlier notice of the information to be included in the Certificate.

A Subscriber must not create Digital Signatures using a Private Key corresponding to the Public Key listed in a Certificate (or otherwise use such Private Key) if the foreseeable effect would be to induce or allow reliance upon a Certificate that is deemed not valid.

Upon revocation of a Certificate the Certificate's Operational Period ends/expires and the Subscriber must:

a) cease using the Certificate for any purpose whatsoever; and
b) continue to safeguard their Private Keys unless they destroy their Private Keys;

Upon revocation of a Certificate the underlying contractual obligations between the Subscriber and other PKI Entities are unaffected.

9.6.3.1 Subscriber and/or Key Holder Obligations

The Subscriber and/or Key Holder refers to the individual named within the certificate, including the Individual, Certificate Manager and Authoriser. The Subscriber and/or the Key Holder must:

a) not delegate his or her responsibilities for the generation, use, retention, or proper destruction of his or her Private Keys with the exception of storage of keys for archival purposes and destruction of their Private Keys to a person authorised to perform that act on behalf of the Organisation.
b) ensure that their Private Keys are not compromised;
c) immediately notify the Symantec CA or the RA if they become aware that their Private Key has been compromised, or there is a substantial risk of compromise;
d) ensure that all information provided to the RA in relation to issue and use of their Key Pairs and Certificates is to the best of their knowledge, true and complete;
e) immediately notify the Symantec CA or the RA if there is any other change to their Registration Information, or any other information provided to the Symantec CA or the RA in relation to issue and use of their Keys and Certificates;
f) use Keys and Certificates only for the purposes for which they were issued and within the usage and reliance limitations, as specified in this CP, the Certificate Profile and the Certificate;
g) check the details set out in a Certificate on receipt, and promptly notify the Symantec CA if faulty or improper Registration or Certificate Issuance has occurred;
h) if requested by the RA, provide complete and accurate information in relation to their Registration Information or anything else relating to issue or use of their Keys and Certificates; and
i) use Keys and Certificates only for purposes for which they have the actual authority of the Organisation.

The Key Holder, as a representative of the Organisation, must immediately notify the Symantec CA or the RA if:

a) they cease to be an employee or agent of their Organisation;
b) they cease to be authorised to hold Keys and Certificates on behalf of their Organisation; or
c) their Organisation ceases to belong to the Community of Interest;

9.6.3.2 Organisation Obligations

In the case of Device Certificates and Business Certificates, the obligations of the Organisation must be carried out through an Authoriser.

The Organisation must:

a) ensure that their Key Holders comply with their obligations under this CP and the CPS;
b) provide measures to avoid compromise of their Key Holder's Private Keys;
c) immediately notify the Symantec CA when the Organisation becomes aware that a Key Holder's Private Key has been compromised, or there is a substantial risk of compromise;

d) ensure that all information provided to the Symantec CA or the RA in relation to issue and use of their Key Holder's Key Pairs and Certificates is to the best of their knowledge, true and complete;
e) immediately notify the Symantec CA or the RA if there is any other change to the Registration Information, or any other information provided to the RA in relation to issue and use of their Key Holder's Keys and Certificates.
f) if requested by the RA, provide complete and accurate Registration Information or anything else relating to issue or use of the Keys and Certificates; and
g) where they generate Key Pairs for Key Holders, comply with section 6.

The Organisation must immediately notify the Symantec CA or the RA if:
a) any of their Key Holders cease to be an employee or agent of the Organisation;
b) any of their Key Holders cease to be authorised to hold Keys and Certificates on behalf of the Organisation;
c) the Organisation ceases to belong to the Community of Interest; or
d) there is any other change to the Registration Information, or any other information provided to the RA in relation to issue and use of their Key Holder's Keys and Certificates.

In the case of Device Certificates, Organisations must, through an Authoriser:

a) ensure that only appropriately authorised people perform any of the functions of Authoriser as set forth in sections 1.3.4.1 and 3.2.6 and that the Authoriser performs the functions in compliance with their obligations under this CP and the CPS;
b) ensure that only appropriately authorised people perform any of the functions of Certificate Manager as set forth in sections 1.3.4.1 and 3.2.6 and that the Certificate Manager performs the functions in compliance with their obligations under this CP and the CPS;
c) provide measures to avoid compromise, loss, disclosure, modification or unauthorised use of Private Keys;
d) immediately notify the Symantec CA or the RA if the Device on which the Certificate is installed or the application or service identified by the Certificate is sold, decommissioned, destroyed, lost, sold or otherwise ceases to be under the control of the Organisation;

The Organisation agrees not to copy the Certificate (except for the purposes of backup and Escrow as permitted under this Certificate Policy) or to use the Certificate on more than one Device.

9.6.3.3 Certificate Manager Obligations

In the case of the Device Certificate Request process, a Delegated RA process, the KCO Model and the TRA Model, the Certificate Manager assumes additional responsibilities in the provisioning of digital certificates.

The Certificate Manager is responsible, on behalf of the Organisation, to:

a) vouch for the identity of all representatives for whom additional Business Certificates are requested;
b) accept responsibility for the use of all of its Business Certificates (through, for example, signature of a Subscriber Agreement with the Symantec CA); and
c) accept responsibility for the use of all of Device Certificates issued to the Organisation.

9.6.4 Relying Party Representations and Warranties

Before relying on a Certificate or a Digital Signature, Relying Parties must:

a) validate the Certificate (including by checking whether or not it has been revoked, expired or suspended) and the Digital Signature in accordance with section 9.6.4.1; and
b) ascertain and comply with the purposes for which the Certificate was issued and any other limitations on reliance or use of the Certificate which are specified in the Certificate, the CPS or this CP.

If a Relying Party relies on a Digital Signature or Certificate in circumstances where it has not been validated in accordance with section 9.6.4.1 it assumes all risks with regard to it (except those that would have arisen had the Relying Party validated the Certificate) and is not entitled to any presumption that the Digital Signature is effective as the signature of the Subscriber or that the Certificate is valid.

Relying Parties must also comply with any other relevant obligations specified in this CP including those imposed on the entity when it is acting as a Subscriber.

The following summarises the recognised parameters under which a Digital Signature may be relied upon if:

a) the signature was created during the Operational Period of a valid Certificate (ie prior to the Certificate expiring or being revoked);
b) the Digital Certificate used for signing has the *digitalSignature* bit asserted in the Key Usage extension;
c) such Digital Signature can be properly validated by confirmation of its Certificate chain;
d) the Relying Party has no notice or knowledge of a breach of the requirements of the CPS or this CP by the Signer;
e) the purpose for which the signature is being relied upon is within the purposes or limitations referred to in the Certificate or the relevant Certificate Policy; and
f) the Relying Party has complied with all relevant requirements of this CP.

The use of certificates does not necessarily convey evidence of authority on the part of any user to act on behalf of any person or to undertake any particular act. Relying Parties seeking to validate digitally signed messages are solely responsible for exercising due diligence and reasonable judgment before relying on certificates and digital signatures. A certificate is not a grant from Symantec of any rights or privileges, except as specifically provided in the CPS or this CP.

The Relying Party is hereby notified of the possibility of theft or other form of compromise of a private key corresponding to a public key contained in a certificate, which may or may not be detected, and of the possibility of use of a stolen or compromised key to forge a digital signature to a document. For information regarding private key protection, see the Symantec Gatekeeper Website at *https://symantec-gatekeeper.com.au/repository/.*

The final decision concerning whether or not to rely on a verified Digital Signature rests exclusively with the Relying Party.

9.6.4.1 Digital Signature Validation

Digital Signature validation verifies that the Digital Signature was created by the Private Key corresponding to the Public Key listed in the Certificate of the Subscriber named in the certificate (the 'Signer') and that the associated information has not been altered since the Digital Signature was created. Digital Signature validation confirms both the validity of the signer's Certificate as well as the Digital Signature generated using the signer's Certificate.

Validation of a Digital Signature shall be performed by applications to include the following:

a) Certificate status checking in accordance with section 4.9.6;
b) Calculate a new hash of the signed information by re-applying the hash function as was originally applied by the Signer;
c) decrypt the original hash value supplied by the Signer by using the Public Key contained in the Certificate
d) compare the original hash (step c) against the new hash value calculated in step (b) to confirm that the hash values are equal (equal values denote that the data is unchanged).

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Repository Obligations

The Symantec Gatekeeper repository must ensure timely publication of Certificates and Revocation information as required by this CP.

9.7 Disclaimers of Warranties

9.7.1 General Warranty Disclaimer

Except as set forth in this CP, the CPS and the applicable Subscriber Agreement, and to the extent permitted by applicable law, Symantec disclaims any and all express or implied warranties of any type to any person or entity, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided by Certificate Applicants, Subscribers Relying Parties and other third parties.

9.7.2 Specific Disclaimer

Except as otherwise set forth in this CP, Symantec:

a) Disclaims all liability to any person or entity arising from the verification (i.e., proof of identity) of an individual and/or an organisation under the Known Customer Organisation (KCO) and the Threat and Risk Assessment (TRA) Models.
b) Disclaims all liability to any person or entity, regardless of whether the liability arose from negligence, recklessness, fraud, or willful misconduct, for representations contained in a Certificate so long as the Certificate was prepared in compliance with this CP,
c) Does not warrant the standards or performance of any third party hardware or software.
d) Implicit is an acceptance that, subject to Section 9.7.2 above and Section 9.8.1, Symantec shall be responsible for ensuring proper verification (i.e. EOI) under the formal identity verification model even though part of that process is undertaken by another RA.

9.7.3 Disclaimer of Fiduciary Relationship

Nothing in this CP, the CPS, or the issuing of Key Pairs and Certificates under it, establishes a fiduciary relationship between a PKI Service Provider and an End Entity.

9.8 Limitations of Liability

The liability of an entity referred to in this CP for breach of a contract to which the entity is a party, or for any other common law or statutory cause of action, shall be adjudicated according to sections 9.14 and 9.15 below.

Where a PKI Entity is legally liable to compensate another party, the liability of the first mentioned PKI Entity will be reduced proportionally to the extent that any act or omission on the part of the other PKI Entity contributed to the relevant liability, loss, damage, cost or expense.

The PKI Entities acknowledge that one of the factors that affects their ability to limit their liability is the extent to which they effectively notify the PKI Entity suffering the loss or damage of any limits or limitations on which the entity intends to rely.

The provisions set out in this section shall survive the termination of the relevant contract.

9.8.1 Symantec and RA Provider Liability

Symantec and the Gatekeeper accredited RA exclude all warranties, conditions and obligations of any type from the relationship between Symantec or the RA Provider and any other PKI Entity (including without limitation as a result of operating the Symantec CA or the RA role or the SGR) except:

a) to the extent otherwise provided in this CP; or
b) where a condition or warranty is implied into an agreement by a law, and that condition or warranty cannot be excluded.

In no event will Symantec or the RA Provider be liable for any damages (direct and indirect) if Symantec (or the RA Provider, if any) has issued and managed the Certificate at issue in full compliance with this CP.

In no event will Symantec or the RA Provider be liable for any indirect, special, incidental, or consequential damages or for any loss of profits or revenues, loss of data, loss of use, loss of goodwill, or other indirect, consequential, or punitive damages, whether or not reasonably foreseeable, arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, Digital Signatures, or any other transaction or services related to or offered or contemplated by the CPS or this CP, breach of contract or any express or implied warranty or indemnity under or in relation to any Certificates or the CPS or this CP or otherwise misrepresentation, negligence, strict liability or other tort, even if Symantec or the RA Provider has been advised of the possibility of such damages or should have been aware of such a possibility.

Symantec's and the RA Provider's aggregate liability to a non-Symantec PKI Entity and any and all persons concerning a Certificate for the aggregate of all Digital Signatures and transactions related to that Certificate, shall be limited to AUD50,000.

In the event that Symantec's or the RA Provider's total liability exceeds the amount above, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall Symantec or the RA Provider be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

9.8.2 Liability of the Commonwealth

The AGIMO is only responsible for performing the accreditation process with due care, in adherence to published Gatekeeper Criteria and Policies. The AGIMO is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Certification or Registration Authority as the case may be. The AGIMO accepts no responsibility or liability in relation to transactions conducted using the certificates issued under this CP.

Notwithstanding any other provisions of this CP:

a) the Commonwealth makes no representations, and offers no warranties or conditions, express or implied, in relation to:
    i. the activities or performance of any of the PKI Service Providers which are carried out under, or in relation to, this CP; or
    ii. if relevant, the services or products of a particular PKI Service Providers; and
b) the PKI Entities acknowledge and agree that except to the extent that a Commonwealth Agency is carrying out the role of a PKI Entity (in which case the liability of the Commonwealth will be determined in accordance with the provisions set out in section 9.8), the Commonwealth is not liable in any manner whatsoever whether the Keys or Certificates are used in a transaction with an Agency or not, for any loss or damage caused to, or suffered by any person, including a PKI Entity as a result of:
    i. an entity described in this CP carrying out, or omitting to carry out, any activity described in, or contemplated by, the Approved Documents;
    ii. the Commonwealth carrying out, or omitting to carry out, any activity related to the Gatekeeper accreditation process; or
    iii. a negligent act or omission of the Commonwealth.

9.8.3 Subscriber Liability

9.8.3.1 Individual Subscriber Liability

The Subscriber of Individual Certificates:

a) is solely responsible for the contents of any transmission, message or other document signed using the Subscriber's Private Key;
b) warrants to all Relying Parties that during the Operational Period of the Certificate:
    i. no unauthorised person has ever had access to the Subscriber's Private Key;
    ii. the Certificate will be used exclusively for appropriate and lawful purposes;
    iii. at the time the Digital Signature is created, the Certificate has not Expired or been Suspended or revoked;
    iv. all representations made by the Subscriber or authorised by the Subscriber to the Symantec CA or to the RA, are true;
    v. all information contained in the Certificate is to the Subscriber's knowledge true;
    vi. each Digital Signature created using the Private Key corresponding to the Public Key listed in the Certificate is the Subscriber's Digital Signature;
    vii. the Subscriber will not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Digital Certificate (or any other format of certified Public Key) or Certificate Revocation List, unless expressly agreed in writing with Symantec, and
    viii. when the Subscriber encrypts the hash of a document with the Subscriber's Private Key, in circumstances where the Subscriber's Certificate has not been suspended or revoked, others may act on that as if the Subscriber had hand-signed the document.

9.8.3.2 Organisation Subscriber Liability

The Organisation is responsible and therefore liable for any acts of the Key Holders of Business Certificates in relation to the CPS and this CP, and in particular in relation to the use of Keys and Certificates issued under this CP.

Organisations may make their own arrangements with Key Holders concerning the policies and procedures for use of the Certificates and Keys, and liability provisions.

The Organisation is responsible and therefore liable for any acts of Authorisers and Certificate Managers in relation to the CPS and this CP, and in particular in relation to the use of Keys and Certificates issued under this CP.

The Organisation:

a) is solely responsible for the contents of any transmission, message or other document signed using the Key Holder's Private Key;
b) warrants to all Relying Parties that during the Operational Period of the Certificate, and until notified otherwise by the Organisation that:
    i. no unauthorised person has ever had access to the Key Holder's Private Key;
    ii. the Certificate will be used exclusively for appropriate and lawful purposes;
    iii. at the time the Digital Signature is created, the Certificate has not Expired or revoked;
    iv. all representations made by the Organisation, the Key Holder or authorised by the Organisation or the Key Holder to the Symantec CA or to the RA, is true;
    v. all information contained in the Certificate is to the Organisation's and the Key Holder's knowledge true;
    vi. each Digital Signature created using the Private Key corresponding to the Public Key listed in the Certificate is the Key Holder's Digital Signature;
    vii. the Organisation will not allow the Key Holder to use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Digital Certificate (or any other format of certified Public Key) or Certificate Revocation List, unless expressly agreed in writing with Symantec, and
    viii. when the Key Holder encrypts the hash of a document with the Key Holder's Private Key, in circumstances where the Key Holder's Certificate has not been Suspended or revoked, others may act on that as if the Key Holder had signed the document with the Key Holder's usual signature in the normal way.

To the extent that the Authoriser or the Certificate Manager performs a role in the registration for Business and Device certificates, Organisations are responsible and liable for the use made by Authoriser and Certificate Manager of Certificates and Keys and the instructions issued to the Symantec CA and PKI Entities by the Authoriser and Certificate Manager.

Organisations may make their own arrangements with Authorisers and Certificate Managers concerning the policies and procedures for use of the Certificates and Keys and for providing issuing and revocation instructions to the Symantec CA and PKI Entities, and liability provisions (see Appendix C).

9.8.4 Liability Under the KCO and TRA Model

To the extent a PKI Entity performs a role in the verification (i.e., proof of identity) of Certificates under the KCO or TRA Model:

(1) that entity is responsible and liable for the identification and authentication of Subscribers and the accuracy of the certificate information provided; and
(2) That entity shall indemnify Symantec for any loss, damage, and expense of any kind, arising out of or in connection with any negligence, falsehood, or misrepresentation of fact conveyed to Symantec.

9.8.5 Relying Party Liability

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

a) To the extent permitted by applicable law, Individual Subscribers shall indemnify CAs or RAs for and loss, damage and expense of any kind, arising out of or in connections with:

- Any falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Any 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,
- Any failure by the Subscriber 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 unauthorised use of the Subscriber's private key,
- 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,
- The manner and extent of the use or publication of the Subscriber's Certificate except to the extent that the use or publication of the Key Holder's Certificate was caused by the Symantec CA or the RA using or publishing the Key Holder's Certificate other than as allowed by this CPS,
- The Subscriber's negligence or willful misconduct.

b) To the extent permitted by applicable law, Organisation Subscribers shall indemnify the Symantec CA and the RA for any loss, damage and expense of any kind, arising out of or in connection with:
   - the manner and extent of the use or publication of the Key Holder's Certificate except to the extent that the use or publication of the Key Holder's Certificate was caused by the Symantec CA or the RA using or publishing the Key Holder's Certificate other than as allowed by this CPS;
   - the Organisation's or the Key Holder's negligence or willful misconduct;
   - any falsehood or misrepresentation of fact by the Organisation or the Key Holder (or any person acting on the Organisation's instructions);
   - the Organisation's or the Key Holder's failure to disclose a material fact, if the misrepresentation or omission was made negligently or with the intent to deceive the Symantec CA or the RA or any person receiving or relying on the Key Holder's Certificate; or
   - any failure by the Organisation or the Key Holder to protect the Key Holder's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the key, except to the extent that the Subscriber's Private Key or Certificate has been compromised by Symantec's or the RA's willfully wrongful, fraudulent or negligent conduct.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify 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.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

The CP becomes effective upon approval by the AGIMO and publication in the Symantec Repository. Amendments to this CP become effective upon approval by the AGIMO and publication in the Symantec Repository.

9.10.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version. Termination of the CA or RA shall be conducted in accordance with section 5.8.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, Symantec Gatekeeper participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. Termination of the CA or RA shall be conducted in accordance with section 5.8.

9.11 Individual Notices and Communications with Participants

Notices to Subscribers must be sent to the physical, postal, facsimile or email address of the Subscriber, which is included in its Registration Information, or to another address which the Subscriber has specified to the sender.

Requests to the Symantec GK PKI must be sent to the physical, postal, facsimile or e-mail address as set out on the Symantec Gatekeeper website, or to another address which Symantec has specified to the sender.

A notice to any entity in relation to this CP must be signed by the sending entity. If the notice is sent electronically it must be digitally signed.

Depending on the delivery mechanism, a notice is taken to be received:

a) at the time delivery occurs whether or not any person is there to receive it (if hand-delivered to a physical address);
b) at 5pm on the third day after it is posted even if the notice is returned to the sender (if posted by prepaid post);
c) when the sending machine produces a report showing the transmission was successful (if transmitted by facsimile); and
d) when it enters a system under the control of the addressee (if sent by e-mail).

A notice that is taken to be received at the addressee's place of business outside normal business hours, the parties agree in these circumstances that it is actually taken to be received at that location at 9 am on the next business day.

9.12 Amendments

9.12.1 Procedure for Amendment

The following process describes how changes to an Approved Document (including this CP and the CPS) may be affected:

a) the change request is formulated and submitted to the Policy Approval Authority, which reviews the change request in terms of the impact (if any) on the operation of the Symantec CAs and/or RAs, assesses the justification, and if it deems it necessary, returns the change request with comments suggesting any further work required before the request is submitted to the Gatekeeper Competent Authority;
b) on determining that the change request is suitable for submission to the Gatekeeper Competent Authority, a copy of the requested changes (clearly explained and documented) are forwarded to the Gatekeeper Competent Authority along with any supporting documentation that the Policy Approval Authority deems appropriate for the proper consideration of the change request;
c) the Policy Approval Authority is responsible for liaising with the Gatekeeper Competent Authority to ensure the timely consideration of the change request;
d) a change shall only be made to the Approved Documents following approval granted by the Gatekeeper Competent Authority; and
e) the Symantec CA will update the Repository to reflect the current version of all publicly accessible Approved Documents so that End Entities can obtain current versions of all publicly accessible Approved Documents.

New documents for which approval is sought must follow the same process above, however instead of providing details of a change request, the new document must be provided to the Policy Approval Authority for approval.

9.12.2 Notification Mechanism and Period

The Symantec CA shall maintain all publicly accessible Approved Documents in the Repository. A summary of changes to all publicly accessible Approved Documents shall also be published in the Repository.

The Symantec CA will inform any of its PKI Service Providers of all changes to Approved Documents directly, and will use reasonable endeavors to do this.

9.12.3 Circumstances under Which OID must be Changed

If a change is made to this CP that materially affects the assurance provided, then it may be necessary for the Symantec CA to modify the Certificate Policy Object Identifier. If this occurs, the Symantec CA will contact affected Subscribers.

9.13 Dispute Resolution Provisions

If a dispute arises between any PKI Entity (Dispute), either PKI Entity to the Dispute may by written notice to the other PKI Entity specify the details of the Dispute (Dispute Notice). If a Dispute Notice is given, then the PKI Entity must promptly meet and negotiate in good faith to resolve the Dispute.

If the Dispute remains unresolved 30 days after receipt of the Dispute Notice, the PKI Entities agree to submit the Dispute to mediation administered by, and in accordance with, the mediation rules of the Australian Commercial Disputes Centre (ACDC). A single mediator will be agreed by the PKI Entities or, failing agreement, appointed by the ACDC. The Mediation will be held in Melbourne and be subject to the laws in force in the Australian Capital Territory, Australia.

This section does not apply where both PKI Entities to the dispute are Agencies.

A PKI Entity may be legally represented in any mediation.

The Symantec CA must notify the Gatekeeper Competent Authority before commencing legal proceedings against any Subscriber where the Symantec CA is aware that Keys and Certificates have been issued to the Subscriber for the purpose of facilitating electronic transactions with an Agency.

Nothing in this section prevents a PKI Entity from seeking urgent equitable relief before an appropriate Court.

9.14 Governing Law

This CP and the CPS are governed by, and are to be construed in accordance with, the laws from time to time in force in the Australian Capital Territory, Australia.

9.15 Compliance with Applicable Law

The PKI Entities agree to submit to the jurisdiction of the courts having jurisdiction within the Australian Capital Territory, Australia.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability, Survival, Merger

Any reading down or severance of a particular provision does not affect the other provisions of this CP or the CPS.

Provisions described as having an ongoing operation survive the termination or expiration of the relevant contractual relationship between any PKI Entities.

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

The failure of any PKI Entity to enforce a provision herein shall in no way be interpreted as a waiver of its rights under this CP.

9.16.5 Force Majeure

A PKI Entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in the CPS or this CP if such delay is due to Force Majeure.

If a delay or failure by a PKI Service Provider to perform its obligations is due to Force Majeure, the performance of that entity's obligations is suspended for a reasonable duration commensurate with the Force Majeure event.

If delay or failure by a PKI Service Provider to perform its obligations due to Force Majeure exceeds 30 days, the PKI Entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non-performing PKI Service Provider by providing notice to that PKI Entity in accordance with this CP. If the arrangement, agreement or contract is terminated, then the non-performing PKI Service Provider shall refund any money paid for services not rendered (if any) by the non-performing PKI Service Provider.

9.17 Other Provisions

9.17.1 Conflict of Provisions

To the extent of any conflict between the following documents the first mentioned document shall govern:

a) this CP;
b) the CPS;
c) the Symantec Gatekeeper 2.0 Subscriber Agreement;
d) another agreement between the parties as to the manner and provision of the services described herein;
e) another Approved Document; and
f) a document that is not an Approved Document.

APPENDIX A: ACRONYMS AND DEFINITIONS

Acronyms

The following table provides the literal description of acronyms used throughout this document.

Term	Definition
AES	Advanced Encryption Standard
AGIMO	Australian Government Information Management Office
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CMA	Certificate Management Authority
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Objects Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic curve Digital Signature Algorithm
EOI	Evidence of Identity
GPC	Gatekeeper Policy Committee
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
IETF	Internet Engineering Task Force
ISO	International Organisation for Standards
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAA	Policy Approval Authority
PCA	Policy Creation Authority
PIN	Personal Identification Number
PKAF	Public Key Authentication Framework
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TA	Trusted Agent
TLS	Transport Layer Security

Table 7: Table of Acronyms

Definitions

The following table provides definitions of technical terms used throughout this document. In addition the Symantec Gatekeeper Glossary provides additional Gatekeeper terminology.

Term	Definition
access	Ability to make use of any information system (IS) resource.
access control	Process of granting access to information system resources only to authorised users, programs, processes, or other systems.
Administrator	A Trusted Person within the organisation of a Processing Centre, Service Centre, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. The applicant enters the details to appear in the Certificate.
archive	Long-term, physically separate storage.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
authenticate	To confirm the identity of an entity when that identity is presented.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorisation to receive specific categories of information.
backup	Copy of files and programs made to facilitate recovery if necessary.
binding	Process of associating two related elements of information.
biometric	A physical or behavioral characteristic of a person.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Applicant	An individual or organisation that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorised 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 Authority (CMA)	A Certification Authority or a Registration Authority.
certificate-related information	Information submitted during registration that is included in the certificate. Only a subset of registration information is included in the certificate. For example, while postal and email addresses are submitted for registration, only the email address is included within the certificate. See Registration Information.
Certificate Policies (CP)	This document, which is entitled "Gatekeeper General Category Certificate Policies" and is the principal statement of policy governing the Symantec Gatekeeper PKI.
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 in accordance with CP § 3.4. 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 authority trusted by one or more users to create and assign certificates.
Certification Practice Statement (CPS)	A statement of the practices that Symantec employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
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.
client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Compliance Audit	A periodic audit that the Gatekeeper PKI component undergoes to determine its conformance with Policies that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorised disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise

Term	Definition
	is a loss, theft, disclosure, modification, unauthorised use, or other compromise of the security of such private key.
confidentiality	Assurance that information is not disclosed to unauthorised entities or processes.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
cryptoperiod	Time span during which each key setting remains in effect.
data integrity	Assurance that the data are unchanged from creation to reception
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
firewall	Gateway that limits access between networks in accordance with local security policy.
impersonation	Requesting and being issued a certificate issued under this CPS based on false or falsified information relating to naming or identity.
integrity	Protection against unauthorised modification or destruction of information.
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 (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 escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
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 Managed PKI Customer using Managed PKI Key Manager.
Local Registration Authority (LRA)	An RA with responsibility for a local community.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
naming authority	An organisational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
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 an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a Gatekeeper Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
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.
Object Identifier (OID)	A specialised formatted number that is registered with an internationally recognised standards organisation; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Offline CA	Gatekeeper Primary CAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
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.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for

Term	Definition
	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.
PKI Entity	An entity described in this CP carrying out any activity described in, or contemplated by this CP or the Approved Documents.
PKI Service Provider	An organisation that enters into an agreement with Symantec Gatekeeper to provide services of a component of the Symantec Gatekeeper PKI. Currently Symantec Gatekeeper establishes an agreement with providers for RA services (referred to as the RA Service Provider).
Policy Management Authority (PMA)	The organisation within Symantec responsible for promulgating this policy throughout the Gatekeeper PKI.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key compromise	A loss, theft or modification, or unauthorised access of a private key corresponding to the public key listed in a certificate governed by this CPS, including without limitation by cryptographic analysis or key extraction.
Public Key Infrastructure (PKI)	The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The Gatekeeper PKI consists of systems that collaborate to provide and implement the Gatekeeper PKI services.
RA Service Provider	See PKI Service Provider.
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.
Registration Information	Information, such as a physical, postal, facsimile or email address of the Subscriber or Key Holder, that is not included in a certificate, but is necessary to complete the transaction to issue the certificate. This information that may also be used by a CA in certificate management.
Relying Party	An individual or organisation 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 organisation acts as a Relying Party.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
revocation	The act or process of prematurely ending the operational period of a certificate effective at a specific date and time.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
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 § 6.2.2.
Secure Server ID	A Class 3 organisational Certificate used to support SSL sessions between web browsers and web servers.
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.
Signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. Also referred to as an Identity Certificate.
Sub-domain	The portion of the Gatekeeper PKI under control of an entity and all entities subordinate to it within the Gatekeeper PKI hierarchy.
Subject	The holder of a private key corresponding to a public key. The term “Subject” can, in the case of an organisational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organisational Certificate, an organisation that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using,

Term	Definition
	and is authorised 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 organisation acts as a Subscriber.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
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	Means, with respect to each pertinent portion of this CPS, Symantec Corporation and/or any wholly owned Symantec subsidiary responsible for the specific operations at issue.
Symantec Repository	Symantec's database of Certificates and other relevant Symantec Gatekeeper information accessible on-line.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trusted Person	An employee, contractor, or consultant of an entity within the Gatekeeper PKI organisation responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within an organisation entity that must be held by a Trusted Person.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
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 recognised in classified government nomenclature.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorised individuals, each capable of detecting incorrect and/or unauthorised procedures with respect to the task being performed and each familiar with established security and safety requirements.
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorisations granted to the subject, are changed by issuing a new certificate.
zeroise	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

Table 8: Table of Definitions

APPENDIX B: REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Identifier	Title	Date
ABADSG	*Digital Signature Guidelines* www.abanet.org/scitech/ec/isc/dsgfree.html	1 August 1996
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html	21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/	5 May 1985
FIPS186-3	*Digital Signature Standard* http://csrc.nist.gov/publications/drafts/fips_186-3/Draft_FIPS-186-3%20_November2008.pdf	March 2006
KCO Listing Requirements	Gatekeeper KCO Listing Requirements www.gatekeeper.gov.au	
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*	January 1999
PKCS-1	*PKCS #1 v2.0: RSA Cryptography Standard* www.rsa.com	1 October 1998
PKCS-12	*Personal Information Exchange Syntax Standard* www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html	April 1997
RFC 2560	*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* http://www.ietf.org/rfc/rfc2560.txt?number=2560	June 1999
RFC3647	*Certificate Policy and Certification Practices Framework, Chokhani and Ford.* *www.ietf.org/rfc/rfc2527.txt*	November 2003
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	May 2008
TRO Listing Requirements	Gatekeeper TRO Listing Requirements www.gatekeeper.gov.au	

Table 9: Table of References

APPENDIX C: RECOMMENDATIONS TO ORGANISATIONS

The Organisation is recommended to put in place appropriate procedures for ensuring a full documentary trail is maintained for the request and issue of Device Certificates.

The following steps outline a model that may be adopted by Organisations for processing a request for Device Certificates.

Step 1
Prior to requesting a Device Certificate, the Certificate Manager must be appointed and issued with a General Business Certificate. The Certificate Manager(s) will vouch for the authenticity and integrity of all requests for Device Certificates for the Organisation.

Step 2
The Certificate Manager will forward to the CA a formal application for a Device Certificate containing information necessary for the creation of a Device Certificate. This information should include:

- unique Device Certificate subject identifying information e.g. router serial number;
- details of the Device Certificate subject (e.g. router model and make);
- purpose for which the Device Certificate will be used (e.g. IPsec device, Organisational e-mail at gateway);
- organisational name and ABN (if applicable); and
- name and contact details of the Certificate Manager.

Step 3
Once the CA has checked and approved the application, the Device Certificate is securely delivered to the Certificate Manager.

An Organisation (through its Certificate Manager) takes full responsibility and associated liability in accordance with the Gatekeeper Core Obligations Policy for the installation, management and use of its Device Certificates. Appropriate Certificate management processes need to be in place to:

- manage how Device Certificates are requested;
- ensure that Device Certificates are allocated to the correct application;
- manage what restrictions are placed on the use of Device Certificates; and
- manage the issue and revocation of Device Certificates.

APPENDIX D: ROOT CA POLICY

The section headings of this Appendix correspond to the section headings prescribed by RFC 3647 for the documentation of Certificate Policy. However, only those headings that pertain to the Symantec Gatekeeper Root CA Policy in this Appendix are included and the remaining headings are excluded, thereby resulting in numbering gaps.

1 Introduction

The Symantec Gatekeeper General Category PKI implements a Root Certification Authority (CA) to provide the Trust Anchor for cryptographic communications using X.509 certificates. The Symantec Gatekeeper Root CA is the highest point of Trust within the Symantec Gatekeeper PKI hierarchy. The Root CA consists of the systems, products and services that both protect the Root CA's private key and manages the subordinate CA X.509 certificates issued from the Root CA.

All controls and procedures stipulated in the body of this CP as applicable to CAs are also applicable to the SGR unless expressly overridden by this Appendix.

1.3 PKI Participants

1.3.1 Certification Authorities

The Root Certification Authority (CA) for this CPS is the "Symantec Gatekeeper Root CA–G2" ("SGR CA") operated by Symantec (Australia) Pty Ltd. The SGR CA signs Symantec Gatekeeper Subordinate CAs which issue End Entity Certificates for Subscribers.

1.4 Certificate Usage

The SGR CA serves as the top level root of trust for the Symantec Gatekeeper PKI Hierarchy and as such is itself the issuer of its own Certificate (it possesses a self-signed Certificate). As the Trust Anchor, the SGR CA Certificate is used to start certification paths and issues only CA Certificates to CAs at the subordinate level of the hierarchy in accordance with the policies of this document. The SGR CA shall not issue end-entity certificates.

4 Certificate Life Cycle Operational Requirements

The SGR CA shall only issue Certificates to an approved subordinate CA within the Symantec Gatekeeper General Category PKI hierarchy. The authorisation for issuance and renewal of a CA Certificate is the purview of the Symantec Gatekeeper PKI technical team in collaboration with the PKI Policy Authority

Due to the nature of the SGR CA as Trust Anchor, all Certificate Life Cycle operations are performed via controlled and audited processes, involving multiple Trusted Role participants within a physically protected facility as described in sections 5 and 6 of the CP.

4.3 Certificate Issuance

Upon CA Certificate Issuance, the Certificate is securely delivered to the subordinate CA named in the CA Certificate confirmed to have possession of the private key corresponding to the signed public key.

4.4 Certificate Acceptance

Installation of the CA Certificate by the authorised operators or representatives of the subordinate CA constitutes Certificate Acceptance. Downloading the CA Certificate by a Relying Party entity constitutes Certificate Acceptance.

4.5 Key Pair and Certificate Usage

Certificate usage shall be consistent with the Key Usage field extensions included in the certificate as per section 6.1.7.

4.9 Certificate Revocation

4.9.1 Circumstances for Revocation

The SGR CA shall revoke a subordinate CA Certificate:

- Upon failure of the subordinate CA to meet its material obligations under this Certificate Policy, any applicable CPS, or any other agreement, regulation, or law applicable to the CA Certificate that may be in force,
- If knowledge or reasonable suspicion of compromise is obtained,
- If it is determined that the Certificate was not properly issued in accordance with this Policy and/or any applicable CPS.

4.9.2 Who can Request Revocation

The CA Certificate revocation request may originate from the Symantec Information Security Team in collaboration with the Policy Authority in response to ongoing security monitoring and investigations.

4.9.4 Revocation Request Grace Period

The request for CA Certificate revocation shall be processed expeditiously. The request for CA Certificate revocation must be investigated and accessed via mechanisms that balance the need to quickly revoke the Certificate for reasons of compromise against the need to prevent unauthorised or unwarranted requests.

5 Facility, Management and Operational Controls

5.1 Physical Controls

When not in operation, all equipment for the offline SGR CA is shut down. When not in use, the SGR CA tokens are placed into secure storage with protection strengths commensurate with the sensitivity of the SGR Trust Anchor.

5.6 Key Changeover

The SGR CA will re-certify its own Certificate.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The SGR CA keys are generated in a Key Generation Ceremony in accordance with Symantec Gatekeeper confidential security policies and multi-person control described in section 6.2.2 of this CP.

6.1.4 CA Public Key Delivery to Relying Parties

The SGR CA's Public Key is made available for download by any relying party entity using mechanisms outlined in section 6.1.4 of this CP.

6.1.5 Key Size

Symantec's SGR and Subordinate CAs shall have a minimum key size equivalent in strength to 2048-bit RSA

6.1.7 Key Usage Purposes

The SGR CA's signing key shall have key usage set for off-line signing of CA Certificates and, optionally, ARLs or other validation service responses..

The subordinate Issuing CA's signing key shall have key usage set for signing end-entity Certificates and, optionally, CRLs or other validation service responses (eg, OCSP responses).

6.2 Private Key Protection

6.2.8 Method of Activating the Private Key

Activation of the SGR CA private key requires that the equipment for the SGR CA be turned on and a threshold of "Secret Shares" be assembled through multi-person controls in accordance with section 6.2.2 of this CP.

6.2.9 Method of Deactivating the Private Key

After completion of a private key operation by the SGR (such as a Key Generation Ceremony), the CA personnel shall remove the SGR CA token(s) from the Reader in order to deactivate them. Once removed from the Reader, tokens shall be protected from unauthorised access and placed into secure storage.

6.3 Other Aspects of Key Pair Management

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The SGR CA Certificate shall be issued with a minimum 4096-bit RSA key length and 25 year certificate validity period.

6.7 Network Security Controls

The SGR CA is operated in an offline (non-networked) mode. Under no circumstances will the server be networked in any fashion.

APPENDIX E: ADDITIONAL EOI MODELS

The section headings of this Appendix correspond to the section headings prescribed by RFC 3647 for the documentation of Certificate Policy. However, only those headings that pertain to the topic of this Appendix, Additional EOI Models, are included and the remaining headings are excluded, thereby resulting in numbering gaps.

The text provided in this Appendix reflects the requirements specified by the Gatekeeper PKI Framework, Evidence of Identity Policy, published by the Australian Government Information Management Office, Department of Finance and Deregulation, February 2009,

1. Introduction

This Appendix describes the following two EOI Models supported by the Symantec Gatekeeper General Category PKI:

- **Known Customer Organisation (KCO) Model** – the Symantec Gatekeeper CA may issue certificates to clients of an Organisation or Agency that is Gatekeeper Listed by the Australian Department of Finance and Deregulation (Finance) under this model of identity verification.
- **Independent Threat and Risk Assessment (TRA) Model** –the Symantec Gatekeeper CA may issue certificates to clients of an Organisation or Agency that is Gatekeeper Listed by the Australian Department of Finance and Deregulation (Finance) under this model of identity verification.

1.3 PKI Participants

1.3.2 Registration Authorities

Under the Known Customer Organisation and the Threat and Risk EOI Models, the KCO and the TRO respectively is Listed by the Gatekeeper Competent Authority through the Gatekeeper Listing process and verifies the identity and the bindings of Subscribers for the issuance of Certificates from Symantec Gatekeeper. The KCO and TRO shall conform to the EOI documentary requirements set forth in the Gatekeeper EOI.

The RA shall supply the correct indication of EOI model and EOI type conducted in identity verification for insertion into the certificate.

1.3.4 Other Participants

1.3.4.1 Known Customer Organisation

The Known Customer Organisation (KCO) is a participant under the Known Customer Organisation (KCO) Model.

A KCO is an Organisation or Agency that has undergone Gatekeeper Listing as a formal acknowledgment that the Organisation has satisfied specific Gatekeeper requirements and will provide the necessary assurance to Relying Parties and Subscribers with regard to the validity of the identity contained within the Certificate.

Under the KCO Model, the principal function of the KCO is to provision Known Customers with digital certificates. The KCO submits requests to the Symantec CA for digital certificates to be issued to the Known Customers of the KCO. The KCO in effect operates as an RA but is not required to undergo accreditation as an RA. While the KCO is not an accredited RA, Gatekeeper Listing requires that the KCO implement security policies and practices equivalent to those of an Gatekeeper accredited RA and the documentation requirements for a KCO in registration processing is also regarded as equivalent to those that are prepared by a RA.

The KCO conducts or holds a pre-existing face-to-face EOI check of their Known Customers in accordance with the Known Customer Standard (AS4860-2007). Under the Known Customer Standard, a face-to-face EOI registration check is not conducted at the time that an application for a Digital Certificate is submitted, but instead, the KCO uses the information collected earlier from a formal EOI check conducted by the KCO (which also meets the requirements of Gatekeeper EOI Policy with respect to the Formal Identity Verification model) within the preceding five years.

The Gatekeeper Listed KCO is required to undergo an annual compliance audit in accordance with Gatekeeper Policies and Criteria attesting their compliance with Gatekeeper Standards. Additional information regarding KCO Listing Requirements can be obtained from the Gatekeeper website http://www.gatekeeper.gov.au

The KCO appoints one or more Certificate Managers for the provisioning of digital certificates within the Organisation.

1.3.4.2 Threat and Risk Organisation

The Threat and Risk Organisation (TRO) is a participant under the Threat and Risk Assessment (TRA) Model.

A TRO is an Organisation or Agency that has undergone Gatekeeper Listing as a formal acknowledgment that the Organisation has satisfied specific Gatekeeper requirements and will provide the necessary assurance to Relying Parties and Subscribers with regard to the validity of the identity contained within the Certificate.

The TRO has undertaken a Threat and Risk Assessment (TRA) that has assessed that the risks associated with the identity verification and management processes combined with any additional risk mitigation strategies implemented by the TRO are either less or equivalent to the Formal Identity Verification EOI Policy.

Under the TRA Model, the principal function of the TRO is to provision digital certificates to individuals and applications/devices. There are no Gatekeeper EOI processes or requirements stipulated for the verification of the identity of individual Key Holders in the TRA model of the General Category. The EOI processes used to issue digital certificates under this EOI model may vary between TROs.

In addition to a TRA conducted by an independent assessor, the Gatekeeper Listed TRO is required to undergo an annual compliance audit in accordance with Gatekeeper policies and criteria. Additional information regarding TRO Listing Requirements can be obtained from the Gatekeeper website http://www.gatekeeper.gov.au

The TRO appoints one or more Certificate Managers for the provisioning of digital certificates within the Organisation.
1.4 Certificate Usage

3 Identification and Authentication

3.2 Initial Identity Authentication

The Symantec CA relies on the following two additional EOI Models for identity validation:

1. **Known Customer Organisation (KCO) Model** – under this model the Symantec Gatekeeper CA may issue General Category Business or Device Certificates to clients of an Organisation or Agency that is Gatekeeper Listed[3] by the Gatekeeper Competent Authority and referred to as a Known Customer Organisation (KCO). This model allows a KCO to submit Certificate Requests to the Symantec CA for the issuance of digital certificates to their *Known Customers*.

   The authorised representative of a Gatekeeper Listed KCO shall present a Gatekeeper Manager Certificate for authentication of the Certificate Request for *Known Customers*. The Symantec CA shall verify the Request to have originated from a duly accredited Gatekeeper KCO and an authorised representative of the KCO based on a valid Gatekeeper Manager Certificate. Upon receipt of a valid Certificate Request from a recognised KCO, the Symantec CA shall issue digital certificates to the *Known Customers* of the KCO identified in the Certificate Request.

   A *Known Customer* refers to an individual associated with and known by the KCO in accordance with the KCO Standard and the Gatekeeper KCO Listing Requirements. Two elements of the identity of a Known Customer are attested by the KCO including: 1) that the Organisation is known, and, 2) that the individual representing the Organisation is known.

2. **Threat and Risk Assessment (TRA) Model** – under this model the Symantec Gatekeeper CA may issue Business or Device Certificates to clients of an Organisation or Agency that is Gatekeeper Listed[4] by the Gatekeeper Competent Authority and is referred to as a Threat and Risk Organisation (TRO).

   The authorised representative of a Gatekeeper Listed TRO shall present a Gatekeeper Manager Certificate for authentication of the Certificate Request. The Symantec CA shall verify the Request to have originated from a duly accredited Gatekeeper TRO and an authorised representative of the TRO based on a valid Gatekeeper Manager Certificate. Upon receipt of a valid Certificate Request from a recognised TRO, the Symantec CA shall issue digital certificates to the individual or application/device identified in the Certificate Request.

[3] Under the KCO Model, to be "Gatekeeper Listed" by Finance, an Organisation or Agency has demonstrated its compliance with the Known Customer Standard and specific Gatekeeper requirements.

[4] Under the TRA Model, to be "Gatekeeper Listed" by Finance, an Organisation or Agency has demonstrated by means of an independent TRA (performed by a member of the Gatekeeper Audit Panel), that its internal EOI processes are equivalent to a face-to-face EOI check conducted in accordance with the Gatekeeper EOI Policy.

The end entity Certificate issued shall indicate the EOI model used in identity validation and application processing.

3.2.2 Authentication of Organisation Identity

The Organisation Identity used in the Distinguished Name of the Subscriber is established by the presentation of a Gatekeeper Manager Certificate on behalf of the KCO or TRO. Because the Certificate Manager uses their Gatekeeper Manager Certificate for authentication and authorisation, it can be assumed for the purpose of this CP that the Organisation has been verified.

3.2.5 Non-Verified Subscriber Information

Under the KCO and TRA Models, certificate information supplied by the KCO and the TRO respectively is not verified by the RA.

3.3 Identification and Authentication for Re-Key (Renewal) Requests

3.3.1 Identification and Authentication for Routine Rekey

Under the KCO Model and TRA Model, the KCO and the TRO respectively perform a corresponding identity verification pertinent to their Organisation and submit the Re-Key Request to the Symantec CA. The Symantec CA shall verify the Request to have originated from a duly accredited Gatekeeper Listed KCO or TRO and from an authorised representative of the Organisation based on a valid Gatekeeper Manager Certificate as described in section 3.2 of this CP.

3.3.2 Identification and Authentication for Rekey After Revocation

For the KCO and TRA Models, the Organisation performs the corresponding EOI check procedure pertinent to their Organisation.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.2 Enrolment Process and Responsibilities

The enrolment process varies depending on the choice of EOI Model as summarised in the following table.

EOI Model	Processing
KCO Model	the KCO performs the identity verification pertinent to their Organisation and submits the Request to the Symantec CA. The RA shall verify the Request to have originated from a duly accredited Gatekeeper Listed KCO or TRO and from an authorised representative of the Organisation based on a valid Gatekeeper Manager Certificate.
TRA Model	the TRO performs the identity verification pertinent to their Organisation and submits the Request to the Symantec CA. The RA shall verify the Request to have originated from a duly accredited Gatekeeper Listed KCO or TRO and from an authorised representative of the Organisation based on a valid Gatekeeper Manager Certificate.

Table 10: Enrollment Process by EOI Model

Following the issuance of Gatekeeper Manager Certificate to a Certificate Manager for an Organisation, requests for certificates may be submitted by the Certificate Manager to the same Symantec CA that supplied the Gatekeeper Manage Certificate.