DigiCert Gatekeeper Certification Practices Statement

Version 3.5

06 June 2022

Within the framework described in section 1.1 (diagram), the role of the CA is performed by **DigiCert Australia Pty. Ltd.** a wholly owned subsidiary of DigiCert, Inc.
Registered Office: Level 3, 437 St Kilda Road Melbourne, Australia
Legal representative: DLA Piper
Australian Business Number: 88 088 021 603
Telephone (switchboard): (03) 9674 5500
ISO Object Identifier (OID): 1.2.36.88021603.333.30.1
Corporate web site (information): http://www.DigiCert.com
Certification service web site: https://my.gatekeeper.digicert.com/
E-mail address (information and enquiries): gk-support@digicert.com

DigiCert Gatekeeper Certification Practice Statement

Published date: 10 June 2022

Trademark Notices

Change	Date Released	Doc Version	Change By	Description
1	4 Dec 2017	2.3	L Hansen	DigiCert rebranding
2	1 Jul 2019	3.0	L Hansen	Updated with Digicert Gen 4 information
3	25 Sep 2019	3.1	M Sullivan	Updated with Current GateKeeper standards
4	4 Feb 2020	3.2	M Sullivan	Updated with new Certificate Profiles.
5	11 Jun 2020	3.3	M Sullivan	Updated with EKU and validity.
6	21 Mar 2022	3.4	M Sullivan	Updated profiles for editorial accuracy
7	06 Jun 2022	3.5	M Sullivan	Updated Device EKU fixed formatting error

TABLE OF CONTENTS

1. INTRODUCTION

This document is the DigiCert Gatekeeper Certification Practice Statement ("CPS"). It states the practices that DigiCert Certification Authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the DigiCert Gatekeeper Certificate Policy ("CP").

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

While the CP sets forth requirements that DigiCert Gatekeeper Participants must meet, this CPS describes how DigiCert meets these requirements. More specifically, this CPS describes the practices that DigiCert employs for:

- securely managing the core infrastructure that supports the DigiCert Gatekeeper PKI, and
- issuing, managing, revoking, and renewing DigiCert Gatekeeper Certificates

in accordance with the requirements of the CP.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

1.1 Overview

The DigiCert Gatekeeper PKI issues digital certificates under the Gatekeeper PKI Framework to individuals, organisations and devices for the purpose of conducting online transactions with government agencies.

The DigiCert Gatekeeper PKI supports the Individual and Business Certificates (" Individual" and "Business") as well as the Device Certificates ("Device"). 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.

DigiCert Gatekeeper Certificates are issued under the DigiCert Gatekeeper Hierarchy established under the Gatekeeper Root CA. The PKI hierarchy is depicted in the following diagram.

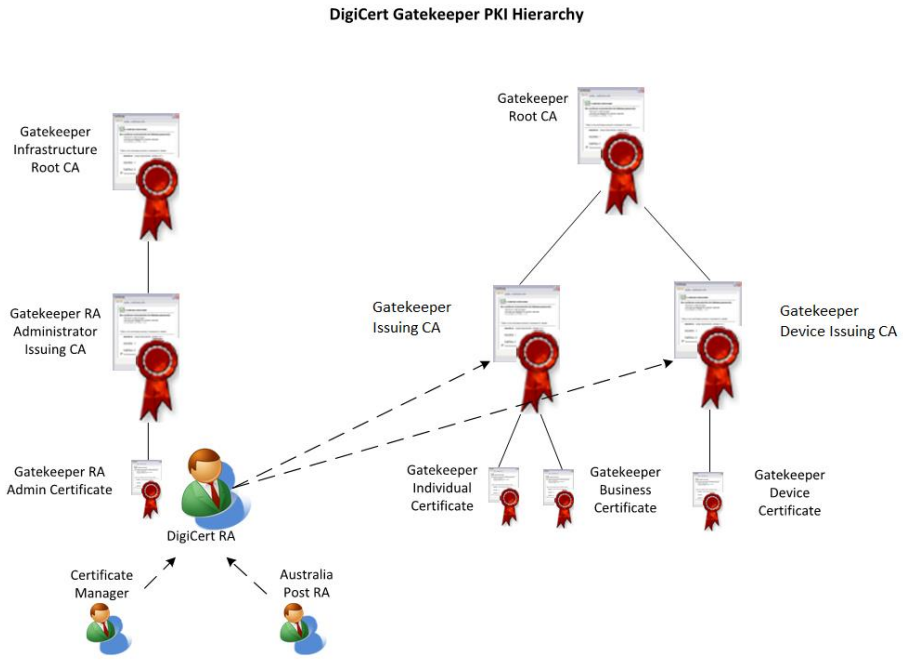

Figure 1: CAs within the DigiCert Gatekeeper PKI Hierarchy

In this CPS, the term “Gatekeeper CA”, refers to an Issuing CA within the PKI hierarchy providing the DigiCert Gatekeeper CA services (inclusive of the combined systems, personnel and processes that perform the functions and provide the services of the PKI).

1.2 Document Name and Identification

This document is the “DigiCert Gatekeeper Certification Practice Statement”. The object identifier (OID) assignment to this CPS document is as follows:

> {iso(1) Member body (2) Au (36) DigiCert Australia (88021603) DigiCert Australia Gatekeeper (333) DigiCert Australia Gatekeeper CPS (30)}

DigiCert provides 3 (three) types of Gatekeeper certificates, namely;

- Individual Certificates
- Business Certificates, and
- Device Certificates

All three certificate types fall under the Gatekeeper CP which is represented in all end-entity certificates with the OID 1.2.36.88021603.333.30.1

1.3 PKI Participants

1.3.1 Certification Authorities

The Root Certification Authority (CA) for this CPS is the “Gatekeeper Root CA–G4” (“GR CA”) operated by DigiCert (Australia) Pty Ltd. The GR CA signs DigiCert Gatekeeper Subordinate CAs which issue End Entity Certificates for Subscribers.

The GR and Issuing CAs uniformly assume the functions and obligations of CAs as outlined in this CPS, however, the GR CA also assumes additional functions and obligations that are distinct for the GR CA alone. The DigiCert Gatekeeper PKI implements a Root Certification Authority to provide a Trust Anchor for cryptographic

communications using X.509 certificates. The GR CA consists of the systems, products and services that both protect the GR CA's private key and manages the subordinate CA X.509 certificates issued from the GR CA.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of the DigiCert CA. The DigiCert RA or another Gatekeeper Accredited RA as an RA Service Provider will perform the functions of the Registration Authority.

Where an RA functioning under this CPS is performed by a person other than the DigiCert RA, that RA will be bound contractually by DigiCert to perform the Registration functions in accordance with the CP and other Approved Documents (see definition of Approved Documents in the Glossary).

Under the Levels of Assurance (LOA) Model, the RA verifies the identity and the bindings of Subscribers through a face-to-face EOI check as stipulated in section 3.2. Identity verification verifies the binding of the physical person to the documented name of the Subscriber or Key Holder. Organisation verification verifies the identity of the Organisation and binds the individual named in the Certificate to the Organisation. The DigiCert RA performs the identity verification of the Subscriber of the Business and Device Certificates (ie, organizations) ; a Gatekeeper accredited Registration Authority performs 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 DigiCert RA is granted privileged access to the CA. Gatekeeper accredited RAs and delegated RAs are not granted privileged access to the CA.

1.3.3 End Entities

The End Entities to which this CPS 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 DigiCert Gatekeeper CPS. The CP and this CPS 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 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..

In terms of registration, the term "applicant" refers to the person who generates the request and provides the details to appear in a Certificate. In many instances the applicant is not the name that appears in the Certificate being issued. Two different terms are used in this CPS to distinguish between these two titles: "Subscriber", is the entity which contracts with DigiCert for the issuance of credentials and; "Subject", is the person or device named in the Certificate to whom the credential is bound.

The Subscriber bears ultimate responsibility for the use of the credential while the Subject is the entity that is authenticated when the credential is presented. Typically, the Subscriber and the Subject are same entity, however, in the case of the Device and Business certificate, they are not. In the issuance of the Device certificate, the organization is the Subscriber, while the device is the Subject; in the issuance of the Business certificate, the organization is the Subscriber, while the key holder is the Subject.

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 DigiCert Gatekeeper PKI. A Relying party may, or may not also be a Subscriber within the DigiCert 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 of the CP.

An Authoriser appoints an individual with the authority to fulfil 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 registration 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 Device 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 Gatekeeper Manager Certificate for authentication to perform their duties and as such is the Subject/Key Holder of the 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 of the CP.

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 DigiCert Gatekeeper Manager Certificate for the purposes of managing additional digital certificates for other employees of the Organisation.

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

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

1. complete, sign and lodge the necessary documentation that provide EOI;
2. under the Delegated RA process, approve additional Business Certificates for the Organisation as required for use by other representatives of the Organisation;
3. undertake the obligations set out in section 9.6.3.3 of the CP 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 DigiCert Gatekeeper Manager Certificate on behalf of the Organisation;
2. Approve Device Certificates for the Organisation as required; and
3. undertake the obligations set out in section 9.6.3.3 of the CP on behalf of the Organisation.

The Certificate Manager role performs the following functions:

1. Accurately identify persons applying for Device Certificates are an authorised representative of the Organisation .
2. Approve issuance of certificates as required
3. Ensure that device keys and certificates are installed on the identified device/application, and
4. 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 DigiCert Gatekeeper Policy Management Authority (PMA) is responsible for maintaining this CPS, the corresponding CP and enforcing the performance of the Compliance Audit for each CA that issues certificates under the CP as depicted in the PKI hierarchy in section 1.1. In developing the content of this CPS, the DigiCert Gatekeeper PMA addresses the requirements of the CP approved by the Gatekeeper Competent Authority.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The Gatekeeper Root CA-G4 ("GR") serves as the top level root of trust for the DigiCert Gatekeeper PKI Hierarchy and as such is the issuer of its own Certificate (a self-signed Certificate). As the Trust Anchor, the GR CA is the starting point in all DigiCert Gatekeeper certification paths, signing DigiCert Gatekeeper Subordinate CAs. The GR does not issue end-entity certificates.

The purpose of the subordinate Issuing CA Certificates and Key Pairs issued under this CPS 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 CPS 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 dependant on the Level of Assurance it has been Validated to this would include:

LOA 1 At this level identity is unique within the intended context. There is little confidence in the accuracy or legitimacy of the claimed identity. Self-claimed or self-asserted identity (including pseudonymity) is possible but not anonymity.
Identity assertions at this level are appropriate for transactions with minimal consequences to Relying Parties from the registration of a fraudulent identity.

LOA 2 At this level identity is unique within the intended context, identity has been asserted by authoritative sources and identity may be used in other contexts. There is some confidence in the claimed identity.
Identity assertions at this level are appropriate for transactions with some minor consequences associated with the registration of fraudulent identity

LOA 3 At this level identity is unique within the intended context, the identity is recognised by authoritative sources, identity information is verified with authoritative sources, identity can be used in other contexts and the Subscriber is linked to the identity. There is high confidence in the claimed identity.
Identity assertions at this level are appropriate for transactions with serious consequences associated with registration of fraudulent identity.

LOA 4 At this level identity is unique within the intended context, the identity is recognised by authoritative sources, identity information is verified with authoritative sources, identity can be used in other contexts and the Subscriber is linked to the identity. There is very high confidence in the claimed identity.
If the Subscriber is an individual then a local, face to face interview is required. This provides greater opportunities for examining the integrity of original identity documents provided as evidence of identity and establishing a link between a Subscriber and a claimed identity.
Identity assertions at this level are appropriate for transactions with very serious consequences associated with the registration of fraudulent identity

The use of DigiCert 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

DigiCert's services under this CPS and the corresponding CP 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.

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

CA certificates may not be used for any functions other than CA functions. End-user Subscriber certificates shall not be used as CA certificates.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

DigiCert Australia Pty. Ltd. (A wholly owned subsidiary of DigiCert, Inc)
ABN: 88 088 021 603
Level 3, 437 St Kilda Road.
Melbourne, Victoria
Phone: +61 3 9674 5500

1.5.2 Contact Person

Enquiries in relation to this CPS should be directed to:

PKI Policy Manager
DigiCert Gatekeeper Policy Management Authority
c/o DigiCert Australia Pty. Ltd. (A wholly owned subsidiary of DigiCert, Inc)
Level 3, 437 St Kilda Road.
Melbourne, Victoria
Phone: +61 3 9674 5500
gk-support@digicert.com

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures (Gatekeeper Accreditation)

The Gatekeeper Competent Authority is responsible for approving the suitability of the CPS and any subsequent changes for compliance with Gatekeeper Accreditation Criteria and granting Gatekeeper Accreditation. The DigiCert

Gatekeeper Policy Management Authority is responsible for maintaining the CPS document for accuracy and compliance and to provide revised documents to the Gatekeeper Competent Authority for subsequent approval.

The DigiCert RA has been granted Gatekeeper Accreditation to verify the identity of organisations, and the DigiCert Gatekeeper CA for the issuance of Certificates and perform the other functions specified in the CPS, in accordance with the CPS.

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 Publication of Certification Information

The DigiCert CA makes the Gatekeeper Root (GR) Certificate and the GR Public Key available to End Entities on the DigiCert Gatekeeper Repository, a publicly available website.

The DigiCert CA maintains the DigiCert Gatekeeper Website at which it publishes or links to:

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

2.2 Time or Frequency of Publication

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

CRLs are issued in accordance with section 4.9.7 of the CP. Where available for that particular Certificate Type, the OCSP Responder provides real time Certificate Revocation status in accordance with section 4.9.9 of the CP.

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

2.3 Access Controls on Repositories

Read only access is provided to the CP, this CPS, and other Approved Documents such as the Subscriber Agreement and Relying Party Agreement, in the DigiCert Repository located at https://gatekeeper.digicert.com/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.

DigiCert has implemented logical and physical security measures to prevent unauthorised persons from adding, deleting, or modifying repository entries.

3. IDENTIFICATION AND AUTHENTICATION

Refer to the DigiCert Gatekeeper Certificate Policy for information regarding authentication for initial registration, Renewal, Reissue and Revocation of Certificates.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

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

Refer to sections 4.1 through 4.9 of the DigiCert Gatekeeper Certificate Policy for operational requirements for initial Certificate Application processing as well as requests for Certificate Re-Key, Reissue and Revocation.

The GR only issues Certificates to an approved subordinate CA within the DigiCert Gatekeeper PKI hierarchy. The authorisation for issuance and renewal of a CA Certificate is the purview of the DigiCert Gatekeeper PKI technical team in collaboration with the PKI Policy Management Authority

Due to the nature of the GR as Trust Anchor, all Certificate Life Cycle operations, as described in section 4 of the CP, are performed via controlled and audited processes, involving multiple Trusted Role participants within a physically protected facility as described in sections 5 and 6.

4.1 Certificate Application

Refer to the DigiCert Gatekeeper CP.

4.2 Certificate Application Processing

Refer to the DigiCert Gatekeeper CP.

4.3 Certificate Issuance

Refer to the DigiCert Gatekeeper CP.

4.4 Certificate Acceptance

Refer to the DigiCert Gatekeeper CP.

4.5 Key Pair and Certificate Usage

Refer to the DigiCert Gatekeeper CP.

4.6 Certificate Renewal

Refer to the DigiCert Gatekeeper CP.

4.7 Certificate Re-Key

Refer to the DigiCert Gatekeeper CP.

4.8 Certificate Modification

Refer to the DigiCert Gatekeeper CP.

4.9 Certificate Revocation and Suspension

Refer to the DigiCert Gatekeeper CP.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

In the revocation of Certificates, the DigiCert CA provides access to digital certificate status information via an approved X.509 compliant protocol (OCSP). CAs are not confined to using a single protocol for the distribution of Certificate information. The CA ensures that information in Directories is synchronised.

The status of public certificates is available via CRL through the DigiCert Gatekeeper website (at a URL specified in the CPS), and via an OCSP responder (where available). The freshness of the CRL information is described in sections 4.9.7 and 4.9.8 of the DigiCert Gatekeeper CP. Applications that interface with the OCSP responder can check the status of certificates in real time without needing to consult the CRL for that CA.

4.10.2 Service Availability

Certificate Status Services are made 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 DigiCert 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 DigiCert 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

DigiCert Gatekeeper CA maintains ancillary confidential documentation that supplements this CPS and the annual Gatekeeper Compliance Audit by providing more detailed requirements for protections in relation to the Confidentiality, Integrity and Availability of the DigiCert Gatekeeper PKI. While such documentation is not made publicly available, they are made available to authorised personnel in the conduct of the annual WebTrust for Certification Authorities audit in accordance with section 8.

DigiCert Gatekeeper CA maintains a Protective Security Plan (PSP) which describes the practices for ensuring the security and integrity of the overall operation of the DigiCert CA, including the establishment of standards for the access and operation of the DigiCert CA's service elements. The Protective Security Plan details those procedures which are necessary to ensure that the DigiCert CA's clients can have the highest possible level of assurance that critical functions have been identified, and have been provided at appropriate levels of trust, in particular, CA Private Key security, key/data recovery (ie. lost keys or legal access), privileged user management, Certificate publication and integrity, key generation and transfer mechanisms.

The Protective Security Plan includes the following elements: System Description; Security Objectives; Data Description; System Users; System Mode; Security Administration; Physical Security; Comsec (Communications Security) Standards; Networking; Logical Access Control; Audit Accountability; Quality Assurance; Configuration Management; System Integrity; Contingency Handling; Education and Training; Control of Removable Media; Maintenance, Sanitizing and Disposal of Hardware and Software; Data Transfer Procedures; Emergency Destruction; and Incident Management.

The DigiCert Gatekeeper facilities conform to the standards and guidelines stipulated by the Defence Signals Directorate Information Security Manual (ISM).

At the commencement of the DigiCert Gatekeeper operations, the Information Security Registered Assessor Program (IRAP) assessor has evaluated DigiCert's security and operations documentation and policies and have confirmed that they meet requirements of the Gatekeeper programme.

The DigiCert CA maintains a configuration management program to manage changes to the DigiCert Gatekeeper CA or RA operations.

5.1 Physical Controls

DigiCert implements physical controls and security to ensure that the DigiCert CA and RA are able to provide their services in a secure, reliable and trusted manner. The Protective Security Plan details the physical controls of the facilities housing the DigiCert CA's systems, including in relation to the following sub-sections.

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

5.1.1 Site Location and Construction

DigiCert's secure facility has been designed to provide 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 zones. A zone 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 Zone provides more restricted access and greater physical security against intrusion or unauthorised access.

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

5.1.2 Physical Access

DigiCert's Gatekeeper CA systems are protected by five zones of physical security, with access to the lower zone required before gaining access to the higher zone.

Progressively restrictive physical access privileges control access to each zone. Sensitive CA operational activity—any activity related to the lifecycle of the certification process such as authentication, verification, and issuance—

occurs within very restrictive physical zones. Access to each zone requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional zones enforce individual access control through the use of two factor authentication. Unescorted personnel, including un-trusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional zones for key management security, which serves to protect both online and offline storage of CA cryptographic hardware (cryptographic signing units or CSU) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets, and containers. The opening and closing of cabinets or containers in these zones is logged for audit purposes.

5.1.3 Power and Air Conditioning

The secure facilities of CAs and RAs is equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities are 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 are constructed and equipped, and procedures implemented, to prevent floods or other damaging exposure to water damage.

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

CAs and RAs protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and use protective containers and 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 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 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 are considered to be “Trusted Persons” serving in a “Trusted Position.” Persons seeking to become Trusted Persons by obtaining a Trusted Position meet the background screening requirements set out in this CPS.

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

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;

- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:
- customer service personnel,
- 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 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 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 includes 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 is further confirmed through background checking procedures specified in this CPS.

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

DigiCert Gatekeeper CAs and RAs 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, DigiCert 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

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

DigiCert Gatekeeper CAs and RAs 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 also periodically review their training programs, and their training address the elements relevant to functions performed by their personnel.

Such training programs must address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of the DigiCert 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

DigiCert Gatekeeper CAs and RAs 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

DigiCert Gatekeeper CAs and RAs 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 are commensurate with the frequency and severity of the unauthorised actions.

5.3.7 Independent Contractor Requirements

DigiCert Gatekeeper 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 are allowed access to the DigiCert secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

The DigiCert CA is required to log particular information.

5.4.1 Types of Events Recorded

The types of auditable events that must be recorded by CAs and RAs are set forth below. All logs, whether electronic or manual, contain the date and time of the event, and the identity of the entity that caused the event.

Types of auditable events 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,
  (6) physical access logs,
  (7) system configuration changes and maintenance (including access passwords and system privileges),
  (8) 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)
- Failed read and write operations on the Certificate and repository
- Changes to Certificate creation policies e.g., validity period.

5.4.2 Frequency of Processing Log

Audit logs are 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 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 are documented.

5.4.3 Retention Period for Audit Log

Audit logs are 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)

The audit system is maintained internally.

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 DigiCert CA complies 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.

DigiCert Gatekeeper practices for general records archival and records retention are included within the Protective Security Plan.

5.5.1 Types of Records Archived

DigiCert Gatekeeper CAs and RAs 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 DigiCert CA is required to archive particular information including documentation of actions and information that is material to each Certificate Application and to its creation. These records include all relevant evidence in their possession regarding:

- the identity of the Applicant named in each Certificate;
- the identity of persons requesting Certificate Revocation;
- other facts represented in the Certificate;
- Time Stamps; and
- any other material facts related to issuing Certificates.

5.5.2 Retention Period for Archive

Audit trail information are kept for a minimum period of seven (7) years from the date of generation. Records related to Certificates (including Personal Information) are retained for at least thirty (30) years after the date the Certificate expires or is revoked.

5.5.3 Protection of Archive

The DigiCert CA and PKI Service Providers maintain records in a trustworthy fashion. The archive of records are 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 are protected either by physical security or a combination of physical security and cryptographic protection. It is also 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 are maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

The following records are Time Stamped:

- Certificates
- CRLs and other Revocation databases
- Customer service messages.

5.5.6 Archive Collection System (Internal vs. External)

The archive collection system is maintained internally.

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 CA's Certificate, the GR 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 either approve or reject the renewal application. If approved, the Superior Entity conducts a Key Generation Ceremony in order to generate a new key pair for the CA. During such Key Generation Ceremony, the Superior Entity signs and issues the CA a new Certificate. New CA Certificates containing the new CA public keys generated during such Key Generation Ceremony are made available to Relying Parties.

In the case of the GR, the GR will re-certify its own Certificate.

5.7 Compromise and Disaster Recovery

DigiCert Gatekeeper maintains a Disaster Recovery and Business Continuity Plan covering all reasonably foreseeable types of disasters and compromises affecting the services under this CPS including:

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

The Disaster Recovery and Business Continuity Plan are consistent with the requirements of the DigiCert CA's Protective Security Plan.

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, are kept in off-site storage and made available in the event of a compromise or disaster. The DigiCert 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 CPS including:

a) loss or corruption (including suspected corruption) of computing resources, software, and/or data of the DigiCert CA or another PKI Service Provider; and
b) Compromise of the DigiCert 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 DigiCert 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, are promptly made by the affected CA or RA in accordance with DigiCert'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 DigiCert CA is compromised, the GR 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

DigiCert develops, maintains, annually tests, and, when necessary, implements a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster on CA and RA operations. 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 CPS.

DigiCert 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 DigiCert 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 CPS.

The DigiCert CA will give as much notice as possible of the relevant circumstances, and the actions the DigiCert CA proposes for the benefit of the DTA, all Subscribers; and the Relying Parties of which the DigiCert CA is aware. Where the DigiCert CA intends to terminate its own services, it will attempt to give at least three months notice to the affected parties.

If a PKI Service Provider (including the DigiCert CA itself) unexpectedly ceases providing services the DigiCert 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 DigiCert CA or any other entity has under the requirements set forth in section 5.7 (Compromise and Disaster Recovery). Each PKI Service Provider shall co-operate with each other in minimizing disruption to the services provided under this CPS to the affected parties.

If any Personal Information is transferred from one PKI Service Provider to another during the process of termination, each relevant PKI Service Provider shall ensure that the information is protected in accordance with section 9.3 and 9.4 of the CP.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The DigiCert Gatekeeper CA maintains the Key Management Plan, which specifies technical security controls on generation, distribution and use of its own CA Key Pairs. CA keys are generated in a Key Generation Ceremony. All Key Generation Ceremonies are conducted in accordance with DigiCert Gatekeeper confidential security policies. A trustworthy hardware device operating within a processing centre is used to create, protect, and store each Subordinate CA Private Keys.

The DigiCert CA Key Pairs are generated using algorithms that comply with the standards described in the Defence Signals Directorate Information Security Manual (ISM). The GR CA keys are generated in a Key Generation Ceremony in accordance with DigiCert Gatekeeper confidential security policies and multi-person control described in section 6.2.2 of the DigiCert Gatekeeper CP.

The DigiCert CA does 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.

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. 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 by the Defence Signals Directorate Information Security Manual (ISM).

6.1.2 Private Key Delivery to Subscriber

The DigiCert CA does not deliver its CA Private Keys to any entity. As the Subscriber's Private Keys are generated and stored by the Subscriber's application (eg a browser), there is no need for the DigiCert 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 DigiCert 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 DigiCert CA as part of the Key Generation process. When a Public Key is transferred to the DigiCert CA to be certified, it is 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 DigiCert CA publishes a copy of the Certificate in the Certificate Directory and in other appropriate locations, as determined by the DigiCert CA.

6.1.4 CA Public Key Delivery to Relying Parties

The DigiCert 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 GR CA's Public Key, and the Public Keys of all Subordinate CAs, will be made available for download via the Repository.

6.1.5 Key Sizes

The GR and Subordinate CA Keys are 3072 bits or longer. The DigiCert Gatekeeper 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.

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 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 Device certificate type, dual-use Device Certificates are issued with Key Usage set to *DigitalSignature, KeyEncipherment* and *DataEncipherment*.

The GR CA's signing key have key usage set for off-line signing of CA Certificates and, optionally, ARLs or other validation service responses. The subordinate CA's signing key has key usage set for signing end-entity Certificates and, optionally, CRLs or other validation service responses.

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.

DigiCert 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 DigiCert Gatekeeper PKI are protected using a Trustworthy System. The DigiCert Gatekeeper CAs perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-1 level 3 and has been evaluated at the CCS Common Criteria EAL4+ assurance level assurance.

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 of the DigiCert Gatekeeper CP.

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

Both the operational and backup versions of DigiCert 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.

DigiCert utilises Secret Sharing (multi-person control) to protect the activation data needed to activate the CA private keys in accordance with the DigiCert 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) are required to operate the private key.

The DigiCert CA enforces a threshold of three (3) shares needed 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

DigiCert Gatekeeper does not perform Key Escrow.

6.2.4 Private Key Backup

DigiCert backs up the CA private keys to enable recovery from disasters and equipment malfunction in accordance with DigiCert Gatekeeper confidential security policies. Back-ups are 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 are protected from unauthorised modification or disclosure through physical or cryptographic means. Backups 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. Subscribers are advised not to back up their Private Keys used for Signing.

The DigiCert 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

The DigiCert CA keeps a copy of all Private Keys it has historically used 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 are not 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 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 are performed securely to the extent necessary to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private keys. Such transfers are limited to making backup copies of the private keys on tokens in accordance with DigiCert Gatekeeper confidential security policies. Private keys are 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 by using the secure export/import capabilities of PKCS#12 protocols together with procedural security measures that prevent unauthorised persons from gaining access to the 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, DigiCert RAs 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 persons 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 remove the token containing such CA's private key from the Reader in order to deactivate it. With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA personnel remove the token containing such CAs' private keys from the Reader in order to deactivate them. Once removed from the Reader, tokens are protected from unauthorised access and placed into secure storage.

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). CA personnel decommission the CA's private key by deleting it using functionality of the token containing such CA's private key so as to prevent its recovery following deletion, while not adversely affecting the private keys of other CAs contained on the token. Such a process is witnessed in accordance with DigiCert 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

DigiCert Gatekeeper archives its CA public keys. No stipulation for Subscribers.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The GR CA Certificate with 4096-bit RSA key length is issued with a 30-year certificate validity period. The GR will certify or re-certify all DigiCert Gatekeeper Subordinate CA Certificates, giving DigiCert Subordinate CAs a 15 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 DigiCert 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 thereafter ceases 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 is set according to the time limits set forth in the following table.

Certificate Type:	***Validity Period***
Individual Encryption and Individual Signing Certificates	Up to 30 months.
Business Encryption and Business Signing Certificates	Up to 30 months.
Device Certificate	Up to 30 months.

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 DigiCert CA generates activation data for their CAs' private keys and RAs, in accordance with the Secret Sharing requirements of this CPS and the DigiCert Gatekeeper confidential security policies. The DigiCert 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 DigiCert for authentication of the Subscriber for download of the certificate at issuance. Subscribers 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 DigiCert CA utilises Secret Sharing in accordance with this CPS and the DigiCert 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. Shareholders do not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorised use of it whatsoever; or
- disclose his, her, or any other person's status as a Shareholder to any third party.

The installation codes generated by DigiCert 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 DigiCert Gatekeeper confidential security policies.

6.5.1 Specific Computer Security Technical Requirements

DigiCert ensures 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 do not have accounts on the Production servers.

The CA have Production networks logically separated from other components to prevent network access except through defined and authorised application processes. DigiCert uses firewalls to protect the Production network from internal and external intrusion and limit the nature and source of network activities that may access Production

Systems. DigiCert requires the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and requires that passwords be changed on a periodic basis and whenever necessary. Direct access to a CA database containing the CA Repository is limited to Trusted Persons in DigiCert's operations group having a valid business reason for such access.

RAs ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorised access. RAs logically separate access to these systems and this information from other components to prevent access except through defined and authorised processes. RAs use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and as necessary. Direct access to the RA's database maintaining Subscriber information is limited to Trusted Persons in the RA's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

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

6.6.1 System Development Controls

Applications are developed and implemented by DigiCert in accordance with DigiCert systems development and change management standards. Such developed software, when first loaded, provides a method to verify that the software on the system originated from DigiCert, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

DigiCert has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. The configuration, including modifications and upgrades of DigiCert PKI components shall be documented.

DigiCert has mechanisms for detecting unauthorised modification to the software or configuration of DigiCert PKI components.

Systems hosting the DigiCert Issuing CAs only have applications or component software or hardware installed that are directly related to the operation of the DigiCert PKI.

6.6.3 Life Cycle Security Controls

Equipment (hardware and software), including modifications and upgrades, procured for the DigiCert PKI are:

- purchased through a mechanism that reduces the likelihood that any particular component was tampered with
- shipped or delivered via controlled methods that provide a continuous chain of accountability from its origin to its destination and handover to DigiCert, and
- deployed using DigiCert authorised personnel

6.7 Network Security Controls

CA and RA functions are performed using networks secured in accordance with DigiCert Gatekeeper confidential security policies to prevent unauthorised access, tampering, and denial-of-service attacks. In general, the DigiCert CA

uses firewalls for securing network access. Communications of sensitive information are protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

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

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries 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

7.1.1.1 Individual Certificate

The Certificate Profile for the **Individual Dual Key Certificate**, **Individual Encryption Certificate** and the **Individual Signing Certificate**[1] is as follows:

Type	Mandatory	Critical	Value
Subject Distinguished Name	Y	N	*[Example values in italics. For full details see **section 3.1** of the CP.]* **E=***rsmith@xyz.com.au* rfc822 email address of type IA5String. Ideally rfc822Name should be in the *SubjectAltName*) **CN=***Richard Smith* (common name of the Key Holder) **OU=***"Encryption Certificate" or "Signing Certificate" or "Dual Key Certificate"* **L=***Melbourne* **S=***Vic*
Issuer Distinguished Name	Y	N	CN=DigiCert Gatekeeper Issuing CA OU=Gatekeeper PKI O= DigiCert Australia Pty. Ltd.
Version	Y	N	2 (Version 3 certificates)
Serial Number	Y	N	Serial number value
Signature Algorithm	Y	N	Sha256RSA
Subject Public Key Information	Y	N	min RSA 2048 bit key
Valid From	Y	N	day/month/yyyy hh/mm/ss
Valid To	Y	N	day/month/yyyy hh/mm/ss
Authority Key Identifier	N	N	Set (sha256 hash of issuer's Public Key)
Subject Key Identifier	N	N	Set (sha256 hash of Public Key)
Basic Constraints	Y	Y	CA: FALSE Max Path Len: N/A (critical)
Key Usage	Y	Y	*[For Dual Key Certificate]* DigitalSignature, KeyEncipherment, DataEncipherment *[For Signing Certificate]* DigitalSignature *[For Encryption Certificate]* KeyEncipherment, DataEncipherment
Extended Key Usage	N	N	OID: 1.3.6.1.5.5.7.3.2 ClientAuth OID: 1.3.6.1.5.5.7.3.4 emailProtection
Certificate Policies	Y	N	[1]OID: 1.2.36.88021603.333.30 (CPS) [1,1]OID: 1.3.6.1.5.5.7.2.1 (Policy Qualifier) CPS Pointer (URI): https://gk.pkiauth.com.au/cps/ [1,2]OID: 1.3.6.1.5.5.7.2.2 (User Notice) Notice Text: https://gk.pkiauth.com.au/rpa [2]OID: (Certificate Policy) [2,1]OID: 1.3.6.1.5.5.7.2.2 (User Notice) Notice Text: Issued under DigiCert Australia Pty. Ltd. Gatekeeper PKI CP. Refer to https://gk.pkiauth.com.au/about for more information.
Subject Alt Name	N	N	RFC822 name = rsmith@*xyz.com.au*
CRL Distribution Point	Y	N	URL=http://crl.gk.pkiauth.com.au/<JurisdictionName>/LatestCRL.crl

[1] The Certificate profiles for the Dual key. Individual Encryption and Signing Certificates are identical with the exception of the Key Usage extension and Subject OU=<Encryption/Signing Certificate> value.

Private Extension (EOI Assurance Type)	N	N	OID 1.2.36.1.333.5 1 (LOA 1) 2 (LOA 2) 3 (LOA 3) 4 (LOA 4)
Authority Information Access	N	N	OID 1.3.6.1.5.5.7.48.1 (Online Certificate Status Protocol) URL= http://ocsp.gk.pkiauth.com.au
Thumbprint algorithm		N	Sha256
Thumbprint		N	Thumbprint value

Table 10: Certificate Profile –Individual Dual Key, Encryption and Signing Certificates

7.1.1.2 Business Certificate

The Certificate Profile for the **Business Dual Key Certificate, Business Encryption Certificate** and the **Business Signing Certificate**[2] is as follows:

Type	Mandatory	Critical	Value
Subject Distinguished Name	Y	N	*[Example values in italics. For full details see **section 3.1** of the CP.]* **E=***rsmith@xyz.com.au* (rfc822 email address of type IA5String. Ideally rfc822Name should be in the *SubjectAltName*) **CN=***Richard Smith* (common name of the Key Holder) **OU=***"Encryption Certificate" or "Signing Certificate" or "Dual Key Certificate"* **OU=***Finance Dept (business unit)* **O=***XYZ Ltd (Legal entity name)* **L=***Melbourne* **S=***Vic*
issuer Distinguished Name	Y	N	CN= DigiCert Gatekeeper Issuing CA OU=Gatekeeper PKI O= DigiCert Australia Pty. Ltd.
Version	Y	N	2 (Version 3 certificates)
Serial Number	Y	N	Serial number value
Signature Algorithm	Y	N	Sha256RSA
Subject Public Key Info	Y	N	Min RSA 2048 bit key
Valid From	Y	N	day/month/yyyy hh/mm/ss
Valid To	Y	N	day/month/yyyy hh/mm/ss
Authority Key Identifier	Y	N	Set (sha256 hash of issuer's Public Key)
Subject Key Identifier	Y	N	Set (sha256 hash of Public Key)
Basic Constraints	Y	Y	CA: FALSE Max Path Len: N/A (critical)
Key Usage	Y	Y	*[For Dual Key Certificate]* DigitalSignature, KeyEncipherment, DataEncipherment *[For Signing Certificate]* DigitalSignature *[For Encryption Certificate]* KeyEncipherment, DataEncipherment
Extended Key Usage	N	N	OID: 1.3.6.1.5.5.7.3.2 ClientAuth OID: 1.3.6.1.5.5.7.3.4 emailProtection
Certificate Policies	Y	N	[1]OID: 1.2.36.88021603.333.30 (CPS) [1,1]OID: 1.3.6.1.5.5.7.2.1 (Policy Qualifier) CPS Pointer (URI): https://gk.pkiauth.com.au/cps/ [1,2]OID: 1.3.6.1.5.5.7.2.2 (User Notice) Notice Text: https://gk.pkiauth.com.au/rpa [2]OID: 1.2.36.88021603.333.30.1 (Certificate Policy) [2,1]OID: 1.3.6.1.5.5.7.2.2 (User Notice) Notice Text: Issued under DigiCert Australia Pty. Ltd. Gatekeeper PKI CP. Refer to https://gk.pkiauth.com.au/about for more information.
Subject Alt Name	Y	N	RFC822 name = *rsmith@xyz.com.au*
CRL Distribution Point	Y	N	URL=http://crl.gk.pkiauth.com.au/<JurisdictionName>/LatestCRL.crl
Private Extension (ABN) (optional)	N	N	OID 1.2.36.1.333.1 Value <ABN number (IA5 String)>
Private Extension (Legal Name) (optional)	N	N	OID 1.2.36.1.333.1.1 Value <Legal name of company>
Private Extension (EOI Assurance Type)	Y	N	OID 1.2.36.1.333.3 Values = 1 (Certificate Manager) (as IA5String) 2 (Additional Key Holder)

[2] The Certificate profiles for the Business Dual Key, Encryption and Signing Certificates are identical with the exception of the Key Usage extension.

Private Extension (EOI Assurance Type)	N	N	OID 1.2.36.1.333.5 1 (LOA 1) 2 (LOA 2) 3 (LOA 3) 4 (LOA 4)
Authority Information Access	N	N	OID 1.3.6.1.5.5.7.48.1 (Online Certificate Status Protocol) URL= http://ocsp.gk.pkiauth.com.au
Thumbprint algorithm			Sha256
Thumbprint			Thumbprint value

Table 11: Certificate Profile – Business Encryption and Signing Certificates

7.1.1.3 Device Certificate

The Certificate Profile for **Device Certificates** (Dual Key Encryption Certificate) is as follows:

Type	Mandatory	Critical	Value
Subject Distinguished Name	Y	N	*[Example values in italics. For full details see **section 3.1** of the CP.]* **CN=***user defined eg CCF Email Gateway* **OU=***user defined eg CCF R1 Trial* **O=***user defined eg XYZ Ltd* **S=***Vic* **C =** *AU*
Issuer Distinguished Name	Y	N	CN=DigiCert Gatekeeper Device Issuing CA OU=Gatekeeper PKI O= DigiCert Australia Pty. Ltd.
Version	Y	N	2 (Version 3 certificates)
Serial Number	Y	N	Serial number value
Signature Algorithm	Y	N	Sha256 RSA
Subject Public Key Information	Y	N	min RSA 2048 bit key
Valid From	Y	N	day/month/yyyy hh/mm/ss
Valid To	Y	N	day/month/yyyy hh/mm/ss
Authority Key Identifier	Y	N	Set (sha256 hash of issuer's Public Key)
Subject Key Identifier	Y	N	Set (sha256 hash of Public Key)
Basic Constraints	Y	Y	CA: FALSE Max Path Len: N/A (critical)
Key Usage	Y	Y	DigitalSignature, KeyEncipherment, DataEncipherment
Extended Key Usage	N	N	OID: 1.3.6.1.5.5.7.3.1 ServerAuth OID: 1.3.6.1.5.5.7.3.2 ClientAuth OID: 1.3.6.1.5.5.7.3.4 emailProtection
Certificate Policies	Y	N	[1]OID: 1.2.36.88021603.333.30 (CPS) [1,1]OID: 1.3.6.1.5.5.7.2.1 (Policy Qualifier) CPS Pointer (URI): https://gk.pkiauth.com.au/cps/ [1,2]OID: 1.3.6.1.5.5.7.2.2 (User Notice) Notice Text: https://gk.pkiauth.com.au/rpa [2]OID: 1.2.36.88021603.333.30.1 (Certificate Policy) [2,1]OID: 1.3.6.1.5.5.7.2.2 (User Notice) Notice Text: Issued under DigiCert Australia Pty. Ltd. Gatekeeper PKI Level of Assurance [1 or 2 or 3 or 4]. Refer to https://gk.pkiauth.com.au/about for more information.
Subject Alt Name	Y	N	*[Example value in italics]* RFC822 Name=*rsmith@xyz.com.au* (Mandatory) DNS Name=*device1.domainname.com.au* (Optional)
CRL Distribution Point	Y	N	URL=http://crl.gk.pkiauth.com.au/<JurisdictionName>/LatestCRL.crl
Private Extension (ABN) (optional)	N	N	OID 1.2.36.1.333.1 Value <ABN number (IA5 String)>
Private Extension (Legal Name) (optional)	N	N	OID 1.2.36.1.333.1.1 Value <Legal name of company>
Authority Information Access	N	N	OID 1.3.6.1.5.5.7.48.1 (Online Certificate Status Protocol) URL= http://ocsp.gk.pkiauth.com.au
Thumbprint algorithm	Y	N	Sha256
Thumbprint	Y	N	Thumbprint value

Table 12: Certificate Profile – Device Certificate

7.1.1.4 Root CA Certificate

The Certificate Profile for the **Root CA Self Signed Certificate**:

Type	Mandatory	Critical	Value
Subject Distinguished Name	Y	N	**O=DigiCert Australia Pty. Ltd.** **OU = Gatekeeper PKI** **CN=Gatekeeper Root CA–G4**
Issuer Distinguished Name	Y	N	**O=DigiCert Australia Pty. Ltd.** **OU = Gatekeeper PKI** **CN=Gatekeeper Root CA–G4**
Version	Y	N	V3
Serial Number	Y	N	Serial number value
Signature Algorithm	Y	N	Sha256 RSA
Subject Public Key Information	Y	N	min RSA 4096 bit key
Valid From	Y	N	day/month/yyyy hh/mm/ss
Valid To	Y	N	day/month/yyyy hh/mm/ss
Subject Key Identifier	Y	N	Set (sha256 hash of Public Key)
Basic Constraints	Y	Y	CA: TRUE Max Path Len: N/A (critical)
Key Usage	Y	Y	Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Alt Name			Directory Address: <DigiCert Internal Identifier>
Thumbprint algorithm	Y	N	sha256
Thumbprint	Y	N	Thumbprint value

Table 13: Certificate Profile – Root CA Certificate

7.1.2 Version Number(s)

The DigiCert Gatekeeper Certificates are X.509 Version 3 Certificates.

7.1.3 Certificate Extensions

The DigiCert CA populates X.509 Version 3 Certificates with the extensions indicated in the Certificate Profiles, section 7.1.1.

7.1.4 Algorithm Object Identifiers

DigiCert Gatekeeper Certificates are signed using the following algorithm.

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.5 Name Forms

Certificates issued 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 DigiCert Gatekeeper 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

DigiCert Gatekeeper Certificates issued under this policy contain a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to either the applicable Relying Party Agreement or the CPS.

7.1.9 Policy Qualifiers Syntax and Semantics

DigiCert supports the use of syntax and semantics policy qualifiers as is indicated in the relevant Certificate Profile.

7.1.10 Processing Semantics for the Critical Certificate Policies Extension

The Certificate Policies extension is not critical.

7.2 CRL Profile

The location of the CRL for a Certificate is published in the certificate extension field named “CRL Distribution Point”.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

The location of the OCSP responder for a Certificate is published in the certificate extension field named “CRL Distribution Point”.

7.3.1 Version Number(s)

DigiCert 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 DigiCert CA and RA conducts periodic audits of its operations. Additionally, in accordance with Gatekeeper requirements, the DigiCert PKI undergoes 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 DigiCert 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 Gatekeeper 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 DigiCert Gatekeeper CA or RA was last audited will be published on the DigiCert Gatekeeper Website and may also be published by Finance.

The results of a DigiCert 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 DigiCert Gatekeeper CA and RA operations may be released at the discretion of DigiCert Gatekeeper management.

9. OTHER BUSINESS AND LEGAL MATTERS

Refer to the DigiCert Gatekeeper Certificate Policy for information regarding business and legal matters governing DigiCert's Gatekeeper services.

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
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
DTA	Digital Transformation Agency
ECDSA	Elliptic curve Digital Signature Algorithm
EOI	Evidence of Identity
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 DigiCert 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 CPS, the term "Certificate" refers to certificates that expressly reference the OID of this CPS 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)	The "Gatekeeper Certificate Policies" is the principal statement of policy governing the DigiCert 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)	This document, which is entitled "Gatekeeper Certificate Practice Statement", is a statement of the practices that DigiCert 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

Term	Definition
	of control over, sensitive information may have occurred. With respect to private keys, a Compromise 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.

Term	Definition
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
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 organization that enters into an agreement with DigiCert Gatekeeper to provide services of a component of the DigiCert Gatekeeper PKI. Currently DigiCert Gatekeeper establishes an agreement with providers for RA services (referred to as the RA Service Provider).
Policy Management Authority (PMA)	The organisation within DigiCert 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

Term	Definition
	device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, 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 DigiCert 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.
DigiCert	Means, with respect to each pertinent portion of this CPS, DigiCert, Inc and/or any wholly owned DigiCert subsidiary responsible for the specific operations at issue.
DigiCert Repository	DigiCert's database of Certificates and other relevant DigiCert 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: LOA requirements

Authentication Requirements for Individual Identity Proofing

The *Gatekeeper Public Key Infrastructure Framework V3.1, 10.4* lists the below Identity Verification Requirements for achieving each of the Level of Assurance in 5 objectives.

Requirement	LOA 1	LOA 2	LOA 3	LOA 4
Identity Verification				
Objective 1: Unique in context	Check that the Subscriber is the sole claimant of the identity being claimed.			
Objective 2: Claimed identity is legitimate (commencement of identity deceased identity check)	No stipulation	No stipulation	Verify one of the following: • Australian Birth Certificate • Australian Passport • Immigration Record • Australian Citizenship Certificate • Australian Visa (supported by a foreign passport) • ImmiCard Check the identity is not that of a deceased person by either: • verifying birth certificate with issuing authority, or • check the Fact of Death file	At an in-person interview verify one of the following: • Australian Birth Certificate • Immigration Record • Australian Citizenship Certificate • Australian Visa (supported by a foreign passport) • ImmiCard Check the identity is not that of a deceased person by either: • verifying birth certificate with issuing authority, or • check the Fact of Death file
Objective 3: Operation of the identity in the community over time	No stipulation	Verify one PRIMARY and one SECONDARY piece of evidence	Verify one PRIMARY and one SECONDARY piece of evidence with an authoritative source (e.g. issuing authority)	As per LOA 3 requirements AND provide evidence at an in-person interview

Requirement	LOA 1	LOA 2	LOA 3	LOA 4
Objective 4: Link between the identity and the person claiming the identity	No stipulation	No stipulation – evidence provided to meet Objective 3 is sufficient to meet Objective 4	Verify link between claimed identity and claimant via one of the following: • Manual/visual comparison of a person's face against a photo on a PRIMARY document • Verification of a biometric previously collected • Knowledge based authentication	As per LOA 3 requirements, except that a visual comparison of a person's face or verification of a biometric to occur as part of an in-person face to face interview
Objective 5: Identity is not known to be fraudulent	No stipulation	No stipulation	Check information/records held within the organisation of known fraudulent identities (if such information exists). Once technology permits these checks **SHOULD** also include checks against information on known fraudulent identities held with authoritative sources such as law enforcement and government agencies.	