DigiCert Consortium

Registration Authority Practices Statement (RPS)

Version 1.1

29 July 2019

DigiCert, Inc.
2801 N. Thanksgiving Way, Suite 500
Lehi, UT 84043
+1 801.701.9600
www.digicert.com

Approval Digital Signature Block

Revision History

Version	Date / Status	Revision Details	Author
1.0	9 May 2019	Initial Draft	Shelley Brewer
1.1	29 July 2019	Revisions based on conversion of the DigiCert Private PKI CPS into a CP/CPS document.	Shelley Brewer

TABLE OF CONTENTS

1. INTRODUCTION

For PKI services provided to the various consortiums in which it participates, DigiCert is responsible for performing the Certification Authority (CA) functions, and a Registration Authority is responsible for performing the Registration Authority (RA) functions.

This Registration Authority Practices Statement (RPS) in conjunction with the applicable Certificate Policy (CP) and the DigiCert Private PKI Certificate Policy (CP)/Certification Practices Statement (CPS) defines the practices that the RA uses to fulfill its obligations under the consortium's PKI requirements. Certificates issued by these groups are the basis for a number of security services including authentication, confidentiality, integrity, and non-repudiation. In order for a certificate to be in compliance with appropriate specifications, it shall comply with the reference documents in section 1.6.3.

Note: all subsequent references to DigiCert CP/CPS in this document refer to the DigiCert Private PKI CP/CPS available publicly here: https://www.digicert.com/legal-repository/**.**

1.1 Overview

The requirements in this RPS are a subset of the requirements specified in the DigiCert Private PKI CP/CPS. The format of this RPS is consistent with IETF RFC 3647. In the event of a conflict between the provisions of the RPS and the corresponding CP/CPS, the CP/CPS takes precedence. Section numbers not included in this RPS document are omitted and should be interpreted as no stipulation.

1.2 Document Name and Identification

The DigiCert Private PKI contracts and agreements with the applicable consortium identifies distinct certificate policies distinguished by Policy Object Identifiers (OIDs) for certificates issued to authorized users, groups, administrators, devices, and other Certificate types as specified. These digital certificates provide assurances that the certificate Subscriber's distinguished name is unique and unambiguous within the consortium's domain, and the identity of the Subscriber's organization is based on a comparison of information submitted by the Subscriber against information in business records or databases. These certificates can be used for digital signatures, encryption, and authentication for proof of identity of components that contain the issued certificates and are compliant with the applicable policy specifications. The OIDs included in a certificate indicating how the certificates were validated are specified in the applicable consortium's policy.

1.3.1 PKI Participants

1.3.1.1 Consortium Policy Authority

The consortium stake holders are responsible for authorizing a CA entity to interoperate under the applicable certificate policy. The policy must specify the expectations of the RA operating under their PKI and the requirements around interoperability.

1.3.1.2 PKI Policy Authority

The DigiCert Certificate Policy Authority (DCPA) is responsible for ensuring that RAs are operated in compliance with the reference documents in section 1.6.3.

1.3.1.3 Organization Management Authority

The RA must manage all organizations and for ensuring that all such RA components are operated in compliance with this RPS. This RA management team is responsible for approving the operations of the RA with DigiCert as required by the reference documents in section 1.6.3 and relevant legal agreements.

RA management is also responsible to resolve name space collisions.

1.3.2 Registration

1.3.2.1 Registration Authority (RA)

Designated RA personnel perform the RA functions required to issue a certificate.

A contractual relationship is established by DigiCert with the RA prior to the authorization of the RA to perform any required identity verification.

1.3.3. Subscribers

The Subscriber is the organization named in the Digital Certificate Subscriber Agreement (DCSA). An authorized representative of the Subscriber, acting as a Certificate Applicant, must complete the certificate application process established by The RA. This process includes assertion by the subscriber s that it will use its key and certificate in accordance with the applicable certificate policy. During the process, the RA confirms the identity of the Certificate Applicant and either approves or denies the application. If approved, the RA communicates the approval to the applicable CA and the Subscriber can then request certificates.

Subscribers include any entity authorized to receive a certificate from the RA. The Subject of a certificate is the party named in the certificate. A Subscriber, as used herein, refers to both the Subject of the certificate and the entity that contracted with the RA for the certificate's issuance.

Subscribers are required to adopt the appropriate CP requirements and any additional certificate management practices to govern the Subscriber's practice for requesting certificates and handling the corresponding private keys. The Subscriber agrees to be bound by its obligations through execution of a DigiCert-approved agreement between the Subscriber and RA. This includes the case where the Subscriber has implemented an automated manufacturing process for requesting and issuing end-entity certificates for installation into devices.

1.3.4. Auditors

The PKI participants operating under this CP require the services of other security authorities, such as compliance auditors. Section 8 of this RPS specifies the required audits, audit parameters, and external auditor qualifications.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The use of the certificates permits message integrity checks, confidentiality of communications, and support for non-repudiation.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued.

DigiCert certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation systems, aircraft communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization responsible for administering and determining the suitability of this RPS is DigiCert. Questions or correspondence related to this RPS should be addressed as follows:

DigiCert, Inc.

2801 N. Thanksgiving Way, Suite 500
Lehi, UT 84043
+1 801.701.9600

1.5.4 RPS Approval Procedures

The DCPA is the final approval authority of any proposed changes to this RPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The RA only accepts names that conform to the rules described in the following sub-sections.

3.1.1 Types of Names

The RA may only accept certificates issued with a subject Distinguished Name (DN) that complies with ITU X.500 standards and X.501 distinguished names. Policies on certificate field and extension information are specified in the applicable profile documents.

3.1.2 Need for Names to be Meaningful

RAs may only accept names from subscribers that are meaningful. RAs must use distinguished names to identify the subject (i.e. person, organization, device, or object) or issuer of the certificate and require meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The RA may not accept any requests for anonymous or pseudonymous certificates.

3.1.5 Uniqueness of Names

RAs must ensure the uniqueness of names for all certificates issued within the CA's domain. Name uniqueness is enforced for the entire Subject Distinguished Name of the certificate rather than a particular attribute (e.g., the common name). RAs must identify the method for checking uniqueness of Subject Distinguished Names within its domain in section 3.2.

3.1.6 Recognition, Authentication and Role of Trademarks

Subscribers may not request certificates with content that infringes on the intellectual property rights of another entity.

Th RA may not accept certificate requests knowing that the issued certificate could infringe the trademark of another. The RA investigates any name collisions brought to its attention. If necessary the RA coordinates with and defers to DigiCert for resolution of name collisions within their own space.

3.2 Initial Identity Validation

"Validation" in this context shall mean the RA's determination that a signature issuance requirement is met, the collection and retention of documentation records supporting the determination that the requirement was fulfilled by the requestor of the certificate throughout the lifetime of the certificate, and the ability of the RA to produce such records in response to a proper audit request. The RA may not have connection to the manufacturing data of the equipment that needed for the certificate issuance.

3.2.1 Method to Prove Possession of Private Key

RAs establish that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

The RA verifies proof of private key possession by verifying the Subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR. If the RA generates the key pair on behalf of the Subscriber, proof of possession by the subscriber is not required.

3.2.2 Authentication of Organization Identity

The RA approval process authenticates the identity of the organization named in the respective Digital Certificate Subscriber Agreement and per the reference documents in section 1.6.3.

The RA authenticates the identity of the organization named in the Digital Certificate Subscriber Agreement by confirming that the organization:

- Exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allow it to conduct business;
- Conducts business at the address listed in the agreement; and
- Is not listed on any of the following U.S. Government denied lists: US Department of Commerce' Bureau of Industry and Security Embargoed Countries List, and the US Department of Commerce' Bureau of Industry and Security Denied Entities List.

A required, the RA validates that an FCC ID is indicated certificate signing request, and that the indicated FCC ID is a valid and certified FCC ID authorized for use in in the consortium, according to the applicable certificate policy.

3.2.3 Authentication of Identity

Where applicable, the RA authenticates the identity of the organization named in the respective Digital Certificate Subscriber Agreement and per the reference documents in section 1.6.3.

Where individual vetting is required, the RA authenticates the individual identity of the:

- Representative submitting the Digital Certificate Subscriber Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization;
- Corporate Contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization and can act on behalf of the organization; and
- Administrator listed in the Digital Certificate Subscriber Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization.

3.2.3.1 Authentication for Role-based Client Certificates

The RA may register certificates that identify a specific role that the Subscriber holds instead of a specific individual (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not). These role-based certificates are used when non-repudiation is desired. A sponsor of the role-based Certificates is verified in accordance with Section 3.2.3 above.

3.2.3.1.3 Professional Installer End Entity Certificates

The RA registers a Professional Installer End Entity certificate request using a Professional Installer CA certificate if and only if:

1. The RA validates the Professional Installer End Entity certificate attributes in accordance with the applicable CP;
2. The RA validates that the individual on whose behalf the Professional Installer certificate signing request has been presented is a Certified Professional Installer as vouched for by the Administrator of the CPI Training Program completed by the individual, and that the certificate attributes reflect this identity;
3. The RA validates the unique identifier (CPIR-ID) as presented with the CPI Accrediting Body as consistent with the identifying information in the certificate; and
   The RA enters into a binding user agreement with the entity requesting the Professional Installer certificate to be signed according to the requirements in the applicable certificate policy.

3.2.3.2 Authentication of Devices

The RA may approve Certificates that identify devices that an organization maintains through a human sponsor or through a group.

3.2.3.2.1 Domain Proxy End Entity Certificates

The RA registers a Domain Proxy End Entity certificate request using a Domain Proxy CA certificate if and only if:

1. The RA validates the Domain Proxy End Entity certificate attributes enumerated in accordance with the applicable certificate policy.
2. The RA validates that the entity presenting the Domain Proxy certificate signing request has been certified as a Domain Proxy operator by the FCC, and that the certificate attributes reflect this identity;
3. The RA validates that the entity presenting the Domain Proxy certificate signing request is operating an FCC-certified Domain Proxy and that it has passed all required certification tests; and
4. The RA enters into a binding user agreement with the entity requesting the Domain Proxy certificate to be signed according to the requirements in the certificate policy.

3.2.3.2.2 SAS Provider End Entity Certificates

The RA registers a SAS Provider End Entity certificate request using a SAS Provider CA certificate if and only if:

1. The RA validates the SAS Provider End Entity certificate attributes in accordance with the applicable CP;
2. The RA validates that the entity presenting the SAS Provider certificate signing request has been certified as a SAS Administrator by the FCC, and that the certificate attributes reflect this identity;
3. The RA validates that the entity presenting the SAS Provider certificate signing request has an FCC-certified SAS and that it has passed all related certification tests;
4. The RA validates that the domain endpoints enumerated in the attributes of the certificate are under the control of the SAS Administrator.
5. The RA enters into a binding user agreement with the entity requesting the SAS Provider certificate to be signed according to the requirements in the applicable certificate policy.

3.2.3.2.3 CBSD End Entity Certificates

The RA registers a request using a CBSD Manufacturer CA or a CBSD OEM CA certificate if and only if:

1. The RA validates the CBSD End Entity certificate attributes in accordance with the applicable certificate policy, including the FCC ID in the device identifier (the format of the device identifier serial number may optionally be validated);
2. The RA validates that the entity submitting the End Entity certificate signing request is the entity which has been extended equipment authorization by the FCC for the device on which behalf the certificate signing is requested, according to the criteria established by the certificate policy, and that the certificate attributes reflect this identity;
3. The RA enters into a contractual agreement with the entity requesting the End Entity certificate to be signed according to the requirements in the applicable certificate policy.

3.2.4 Non-Verified Subscriber Information

Non-verifiable information may be included in a certificate such as:

- Organization Unit (OU); and
- Any other information designated as non-verified in the certificate and as permitted in the certificate profiles.

3.2.5 Validation of Authority

The RA's Certificate issuance process must confirm that the:

- Corporate Contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement;

- Representative submitting the Digital Certificate Subscriber Agreement and certificate application is authorized to act on behalf of the organization;
- Administrators listed on the Digital Certificate Subscriber Agreement and certificate application are authorized to act on behalf of the organization; and
- Contacts listed on the Digital Certificate Subscriber Agreement are authorized to act on behalf of the organization.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscribers may request re-key of a certificate prior to a certificate's expiration. After receiving a request for re-key, the RA may approve a new certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the certificate has an extended validity period, the RA may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

CA and Subscriber certificate re-key follow the same procedures as initial certificate issuance in section 3.2. Identity can be established through the use of the device's current valid signature key

3.3.2 Identification and Authentication for Re-Key After Revocation

If issuance of a new certificate is required due to certificate revocation. The Subscriber must go through the initial identity validation process per section 3.2.

3.4 Identification and Authentication for Revocation Request

The RA authenticates all revocation requests received before requesting revocation from the CA. The RA may authenticate revocation requests by referencing the use of the Private Key corresponding to the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATELIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to the RA.

The Certificate Application is a package consisting of the following:

- The Digital Certificate Subscriber Agreement;
- The Subscriber profile containing contact information;
- The Naming Document, which specifies the content to be bound in the certificate; and
- Any associated fees.

4.1.2 Enrollment Process and Responsibilities

The enrollment process, for a Certificate Applicant, includes the following:

- Completing the Certificate Application package;
- Generating a key pair;
- Providing the requested information;
- Delivery of the public key and key pair to the RA;
- Responding to authentication requests in a timely manner; and
- Submitting required payment.

Communication of information can be electronic or out-of-band.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After receiving a certificate application, the RA verifies the application information and other information in accordance with Section 3.2. The RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to DigiCert. After verification is complete, DigiCert evaluates the corpus of information and decides whether or not to issue the certificate. DigiCert considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable.

4.2.2 Approval or Rejection of Certificate Applications

The RA will approve a certificate application if all of the following criteria are met:

- A fully executed Digital Certificate Subscriber Agreement;
- A completed and signed Naming Document (completing all information necessary for the Certificate contents required by the requested certificate profile);
- Successful identification and authentication of all required contact information in the Applicant/Subscriber profile;
- Receipt of all requested supporting documentation; and
- Payment (if applicable) has been received.

The RA will reject a certificate application for any of the following:

- The Applicant fails to execute the required agreement;
- An authorized representative fails to sign the certificate application;
- Identification and authentication of all required information in section 3.2 cannot be completed;
- The Applicant fails to furnish requested supporting documentation;
- The Applicant fails to respond to notices within a specified time; and
- Payment (if applicable) has not been received

The RA only approves a Certificate Application after verifying the applicant meets all requirements listed in the reference documents in section 1.6.3.

4.4 Certificate Acceptance

Before a Subscriber can make effective use of its private key, The RA explains to the Subscriber its responsibilities as defined in CP section 9.6.3.

In the case of the automated issuance of end entity certificates, the Subscriber is the end entity. The manufacturer in this case must ensure that these responsibilities are followed.

At a minimum, a legal agreement specifying the limits on use and trust on the certificate is required.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers are obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate, and use Certificates in accordance with their intended purpose as specified in the applicable legal agreement, this RPS, the reference documents in section 1.6.3, and/or the key usage extensions in the Certificate.

Subscribers are obligated to prevent unauthorized disclosure of their private keys and activation data in accordance with section 6.2.

Subscriber private key usage is specified through the key usage extension in the associated certificate. Per the Digital Certificate Subscriber Agreement, Subscribers must protect their private keys from unauthorized use and agree to discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

DigiCert does not warrant that any third party software will support or enforce the controls and requirements found herein. A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

Relying Parties ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension, if the extension is present. If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be followed.

Relying Parties should assess:

- The restrictions on key and certificate usage (specified in this RPS and the reference documents in section 1.6.3.) are specified in critical certificate extensions, including the basic constraints and key usage extensions.
- The status of the certificate and all the CA certificates in the certificate chain. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to determine whether reliance on a Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

4.7 Certificate Re-Key

Certificate re-key consists of creating a new certificate for a different key pair (and serial number) but can retain the contents of the original certificate's subjectName. Certificate re-key does not violate the requirement for name uniqueness in section 3.1 of this RPS. The new certificate can be assigned a different validity period, key identifiers, and/or be signed with a different key.

4.7.1 Circumstance for Certificate Rekey

Certificates are re-keyed:

- To maintain continuity of Certificate usage;
- For loss or compromise of original certificate's private key; and
- By a RA during recovery from key compromise.

A certificate may be re-keyed after expiration. The original certificate may be revoked, but cannot be further re-keyed.

4.7.2 Who May Request Certificate of a New Public Key

The following may request a certificate re-key:

- The Subscriber of the certificate or an authorized representative of the Subscriber.

4.7.3 Processing Certificate Re-Keying Requests

For certificate re-key, the RA must confirm the identity of the Subscriber in accordance with the requirements specified in section 3.2 for the authentication of an original Certificate Application.

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, the RA verifies the identity and authority of the entity requesting revocation.

The RA revokes Subscriber certificates under the following circumstances:

- The Subscriber or an authorized representative of the Subscriber asks for the certificate to be revoked for any reason whatsoever;
- The Subscriber's private key corresponding to the public key in the certificate has been lost or compromised:
    - Disclosed without authorization; or
    - Stolen.
- The Subscriber can be shown to have violated the stipulations of its subscriber agreement;
- The Digital Certificate Subscriber Agreement with the Subscriber has been terminated;
- There is an improper or faulty issuance of a certificate;
- A prerequisite to the issuance of the certificate can be shown to be incorrect;
    - Information in the certificate is known, or reasonably believed, to be false;

  - Any other circumstance that may reasonably be expected to affect the reliability, security, integrity or trustworthiness of the certificate or the cryptographic key pair associated with the certificate; and/or
  - The Subscriber has not submitted payment when due.
- Identifying information of the Subscriber in the certificate becomes invalid;
- Attributes asserted in the Subscriber's certificate are incorrect;
- The Certificate was issued:
  - In a manner not in accordance with the procedures required in this RPS, the reference documents in section 1.6.3., and/or the associated Certificate Profiles;
  - To a person other than the one named as the Subject of the Certificate; or
  - Without the authorization of the person named as the Subject of such Certificate.
- The Subscriber's organization name changes;
- The RA suspects or determines that any of the information appearing in the Certificate is inaccurate or misleading;
- DigiCert requests that the certificate is revoked because it determines that the continued use of that certificate is harmful to DigiCert, the RA, or any other applicable participating PKI community;
- The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;
- Either the Subscriber's or the RA's obligations under this RPS, the reference documents in section 1.6.3, are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
- The RA finds that in the ordinary course of business that the certificate should be revoked; and
- In exigent and/or emergency situations.

Whenever any of the above circumstances occur, the associated certificate will be revoked and placed on the CRL. Revoked certificates will be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Any appropriately authorized party as defined in the CP, such as a recognized representative of a Subscriber or cross-signed partner, may request revocation of a certificate. The RA may revoke a certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

Revocation requests may be made by:

- The Subscriber of the Certificate or any authorized representative of the Subscriber as verified in section 3.2;
- DigiCert, the RA, or an associated CA Certificate in the Certificate chain for certificates within its domain; and
- The consortium body governing operation of the certificate.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate must identify the date of the request, the certificate to be revoked, the reason for revocation, and allow the requestor to be authenticated. The RA follows and specifies the steps involved in the process of requesting a certificate revocation according to the DigiCert CP/CPS.

Prior to the revocation of a Subscriber Certificate, the RA authenticates the request. Acceptable procedures for authenticating revocation requests include:

- Having the Subscriber log in to their Certificate Requesting Account and revoking their Certificates via their account portal. The Subscriber will submit their request via their online Certificate Requesting Account, which will employ two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN;
- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Such communication must include two or more of the following: telephone confirmation, signed facsimile, signed e- mail, postal mail, or courier service;
- The representative is the Corporate Contact, Administrator, Legal, or Technical contact authenticated in RPS section 3.2.5; and/or
- If requested by the automated RA in the case of the automated issuance of end-entity certificates.

For Certificates handled by the RA, the process for a revocation request as follows:

1. The RA logs the identity of entity making the request or problem report and the reason for requesting revocation.
2. The RA logs the reasons for revocation in the log if the revocation is performed by the RA.
3. The RA may request confirmation of the revocation from the Subscriber or a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
4. If the request is authenticated as originating from the Subscriber, the RA revokes the certificate.
5. For requests from third parties, the RA trusted personnel begin investigating the request and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem;
    b. the number of reports received about a particular certificate;
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.

If the RA determines that revocation is appropriate, the RA revokes the certificate and contacts DigiCert personnel who update the CRL if not done so automatically

DigiCert and associated CAs in the root chain are entitled to request the revocation of Subscriber Certificates within the CA's Subdomain. Prior to revocation, the RA will send a written notice and brief explanation for the revocation to the Subscriber.

4.9.4 Revocation Request Grace Period

Revocation requests should be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance listed in this RPS.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.2 Physical Access

RA system components of the RA is contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to or disclosure of sensitive information.

5.1.7 Waste Disposal

The RA implements procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

The RA media and documentation that are no longer needed for operations will be destroyed in a secure manner. For example, paper documentation must be shredded, burned, or otherwise rendered unrecoverable.

5.2 Procedural Controls

Procedural controls are requirements on roles that perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the PKI will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

5.2.1 Trusted Roles

Personnel acting in trusted roles include personnel involved with identity vetting and the issuance and revocation of certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the DigiCert PKI and RA's operations. The RA maintains lists, including names, organizations and contact information, of those who act in trusted roles, and makes them available during compliance audits.

Employees, contractors, and consultants that are designated to manage the RA's trustworthiness are considered to be "Trusted Persons" serving in "Trusted Positions." Persons seeking to become Trusted Persons must meet the screening requirements of section 5.3.

The RA considers the categories of their personnel identified in this section as Trusted Persons having a Trusted Position. 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 Rekey requests, or enrollment information;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of a repository; and
- The handling of Subscriber information or requests.

Trusted Persons include, but are not limited to, anyone serving as an RA validating and vetting personnel(such as customer service personnel and contractors), and internal auditors.

5.2.1.2 Registration Authority – Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking certificates, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

The RA appoints persons performing RA functions. Such persons are employees of the RA, or authorized contractors, who have undergone RA training, background vetting, and are given credentials to provide PKI credentialing services.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance requirements to determine if the RA is operating in accordance with certificate policies.

5.2.3 Identification and Authentication for Each Role

An individual assigned to a trusted role defined above is required to identify and authenticate himself/herself before the human resources department., with a check of well-recognized forms of identification, such as passports or driver's licenses before being permitted to perform any action set for that role. Identity must be further confirmed through background checking procedures as set forth in the DigiCert Private PKI CP/CPS. Records of such checks must be maintained for audit records.

5.2.4 Roles Requiring Separation of Duties

A person is not assigned to more than one trusted role where separation of duties is required.

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,

2. Those performing backups, recording, and record keeping functions; and

3. Those performing audit, review, oversight, or reconciliation functions.

No individual can have more than one trusted role. The RA has procedures to identify and authenticate its users and ensure that no user identity can assume multiple roles.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Clearance Requirements

The RA requires that personnel assigned to Trusted roles have the requisite background, qualifications, and experience or be provided the training needed to perform their prospective job responsibilities competently and satisfactorily.

The RA is responsible and accountable for the RA operations and ensures compliance with this RPS. The RA's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

5.3.2 Background Check Procedures

The RA verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role.

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 RA will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by an applicable agency.

The RA requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services

Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified).

Background investigations may include a:

- Confirmation of previous employment;
- Check of one or more professional references;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal records (local, state or provincial, and national);
- Check of credit/financial records;
- Search of driver's license records

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 (all subject to and in accordance with applicable law) may include but is not limited to the following:

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

Background checks must be repeated for personnel holding trusted positions at least every five (5) years.

Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned.

5.3.3 Training Requirements

The RA provides their trusted personnel with the requisite on-the-job training needed for their personnel to perform their job responsibilities relating to RA operations competently and satisfactorily.

The RA also periodically review their training programs, and their training addresses the elements relevant to functions performed by their trusted personnel.

The RA maintains records of who received training and what level of training was completed. RA personnel are sufficiently trained prior to performing independent, unattended duties in the following areas:

- Security principles and mechanisms of the PKI and the its environment;
- Hardware and software versions in use for the RA operation; and
- The requirements in this RPS and the corresponding DigiCert Private PKI CP/CPS.

5.3.4 Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. Personnel filling RA roles are made aware of changes in the RA operation. Re-training is provided for any significant change to the operations. Documentation must be maintained identifying all Personnel who received training and the level of training completed.

5.3.6 Sanctions for Unauthorized Actions

Trusted personnel understand that service in the capacity of a trusted position is contingent on successful performance of the security and functional responsibilities commensurate with that trusted position. Personnel who violate the provisions of the RPS are subject to administrative and disciplinary action. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate. Disciplinary actions are commensurate with the frequency and severity of the unauthorized actions. Details are documented in the RA's employee policies.

5.3.7 Independent Contractor Requirements

Contractors fulfilling trusted roles are subject to all requirements specified in this RPS and the DigiCert CP/CPS. The RA must establish procedures to ensure that any subcontractors perform in accordance with this RPS.

5.3.8 Documentation Supplied to RA Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information. The RPS is made available to RAs in the shared company repository.

5.4 Audit Logging Procedures

Audit log files must be generated for all events relating to the security of the RA functions. Where possible, the audit logs must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All RA audit logs, both electronic and non-electronic, must be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

The RA systems require identification and authentication at system log on with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions. All auditing capabilities of the RA operating system and applications are enabled during installation.

The RA enables all essential event auditing capabilities of its RA applications in order to record the auditable events within the reference documents in section 1.6.3. If the RA's applications cannot automatically record an event, The RA implements manual procedures to satisfy the requirements.

For each event, the RA records the relevant:

(i) date and time;

(ii) type of event;

(iii) success or failure; and

(iv) user or system that caused the event or initiated the action.

Event records are available to auditors as proof of RA practices.

RAs record in audit log files all events relating to the security of the RA system applications, including, without limitation:

- Physical Access / Site Security of RA equipment;
- Account Administration;
- System Administrator accounts on the RA equipment, including such records as:
    - Roles and users added or deleted to the RA system;
    - Access control privileges of user accounts;
    - Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles);
    - Attempts to delete or modify audit logs for the RA operations.
- Trusted employee events:
    - Logon and logoff;
    - attempts to create, remove, set passwords or change the system privileges of the privileged users;

  - Unauthorized attempts to the RA system;
  - Unauthorized attempts to access system files;
  - Failed read and write operations on the Certificate.
- Trusted Personnel changes
  - Appointments by human resources; and
  - Removals.
- Token events (if cryptographic modules are used to house the requested Certificate):
  - Serial number of tokens shipped to Subscriber;
  - Account Administrator Certificates;
  - Shipment of tokens; and
  - Tokens driver versions.

5.4.2 Frequency of Processing Log

Audit logs are removed by trusted personnel and monitored periodically to ensure they do not exceed system capacity. Data shall be backed up regularly, placed into a secure container and labeled with the date. Periodic reviews of audit logs shall be conducted by designated security personnel who are not RA vetting and validation trusted personnel. Review of the audit log is conducted at least once every three months. RAs compare their audit logs with supporting manual and electronic logs when any action is deemed suspicious (if manual records are maintained).

5.4.3 Retention Period of Audit Log

Audit logs are retained as archive records in accordance with section 5.5.2 of this RPS.

5.4.4 Protection of Audit Log

The RA system audit logs shall not open for reading or modification by any human, or by any automated process other than those that perform audit processing. Procedures by the RA are implemented to protect archived data from deletion or destruction before the end of the security audit data retention period if the RA has modification access.

5.4.5 Audit Log Backup Procedures

The audit log data is backed up regularly on the same schedule as the rest of the RA equipment to facilitate data recovery (at least monthly).

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may be external to the RA system(external in the case of manual audit logs maintained or other software solutions implemented to meet the requirements of this RPS and applicable certificate policies.

Automated audit processes are invoked at system or application startup and cease only at system or application shutdown. Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the RA notifies DigiCert. DigiCert solely determines whether to suspend the RA's operations until the problem is remedied.

5.5 Records Archival

5.5.1 Types of Data/Records Archived

The RA records include all relevant evidence in the recording entity's possession, including, without limitation:

- Digital Certificate Subscriber Agreements;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- Security audit data (in accordance with Section 5.4.1);
- Certificate Registration and Revocation requests;
- Subscriber identity authentication data as per Section 3.2.3 (both automated and manual);
- Other data or applications to verify archive contents;
- Documentation required by compliance auditors
- Any attempt to delete or modify the Audit logs;
- Appointment of an individual to an RA trusted role;
- Token lifetime (issuance, recovery, destruction, etc.) documentation (if used);
- Compliance Auditor reports;
- Destruction of cryptographic modules (if used);
- Violations of this RPS; and
- All certificate compromise notifications.

The following shall also be included in RA records only in the case of the automated issuance of end-entity certificates:

- Contractual obligations and other agreements concerning operations of the CA System and equipment configuration;
- Records of all actions taken on certificates issued and/or published; and
- Revocation request information.

5.5.2 Retention Period for Archive

Archive records are retained for a period of at least 10 years without any loss of data.

5.5.3 Protection of Archive

Archive media are handled by trusted employees and stored in a secure storage facility. The archive must be protected against unauthorized viewing, modification, deletion, or other tampering. The archive media 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 RPS section 5.5.2 in accordance with the applicable CP and CPS.

5.5.4 Archive Backup Procedures

If the RA is compiling electronic information, that information will be incrementally backed up on system archives. That electronic information back up is performed on a weekly basis. Copies of paper-based records must be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

RA archive records will be automatically time-stamped as they are created. System clocks used for time-stamping will be maintained in synchrony with an authoritative time standard

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.7 Compromise and Disaster Recovery

DigiCert maintains CRL and OCSP access points that the RA and entities relying on the RA can use to access to revocation information. In the event that local RA operations is not available, DigiCert Administrators have the ability to directly access the DigiCert Control Center to revoke certificates.

5.8 RA Termination

The termination of a RA is subject to the contract between the terminating RA and DigiCert. The RA and DigiCert, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Subscribers and Relying Parties.

After termination, the RA initiates execution of end of audit year archival procedures and continues to retain all archive data for the retention period specified in section 5.5.2.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

If the RA provides cryptographic hardware for non-affiliated subscribers, the RA must generate subscriber key pairs for encryption certificates in a FIPS 140 Level 2 validated cryptographic modules. Key pair generation is performed using FIPS 140 validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. Any pseudo-random numbers use and parameters for key generation material are generated by a FIPS-approved method.

6.1.2 Private Key Delivery to Subscriber

Subscriber key pair generation must be performed by the Subscriber or RA. When RAs generate keys on behalf of the Subscriber, Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. If the Subscribers themselves generate private keys, then private key delivery to a Subscriber is unnecessary.

In all cases, the following requirements must be met for key delivery:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key for more than two weeks after delivery of the private key to the Subscriber;
- The Subscriber shall acknowledge receipt of the private key(s);
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers;
- Delivery must be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers;
- The RA maintains a record of the Subscriber acknowledgement of receipt of the token;

If hardware modules are used in the RA Operations, the RA must:

- Be accountable for the location and state of the module must be maintained until the Subscriber accepts possession of it; and
- When RAs generate keys on behalf of the Subscriber, Private keys may be delivered electronically or may be delivered on a hardware cryptographic module that meet the standard as specified in section 6.1.1.

If electronic delivery is used, the RAs must:

- If not automated through DigiCert, RAs must use FIPS 140-2 Level 1 systems and deliver private keys to Subscribers via TLS (or other equivalently secure method) and secure such delivery through the use of a PKCS#8 package or, at the RAs sole discretion, any other comparably equivalent means (e.g., PKCS#12 package) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys; and
- For electronic delivery of private keys, the key material must be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data is delivered using a separate secure channel.

6.1.3 Public Key Delivery to Certificate Issuer

When a public key is transferred to the issuing CA to be certified, it is be delivered through a mechanism validating the identity of the Subscriber and ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key.

The Certificate Applicant delivers the public key in a PKCS#10 CSR or an equivalent method ensuring that the public key has not been altered during transit; and with proof that the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant will submit the CSR via their online Certificate Requesting Account, which employs two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN (this procedure is not applicable in the case of the automated issuance of end-entity certificates).

6.2 Private Key Protection

6.2.1 Cryptographic Module Standards and Controls

Private key holders must take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with the applicable CP and DigiCert Private PKI CP/CPS.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2].

- Subscribers use a FIPS 140-2 Level 1 or higher validated cryptographic module for their cryptographic operations (if issued one by the RA);
- Subscribers of certificates secure keying material as required by the certificate policy.

6.2.3 Private Key Escrow

Subscriber private keys are not escrowed.

6.2.4 Private Key Backup

Device private keys may be backed up or copied but must be held under the control of the Subscriber or other authorized administrator. Backed up device private keys cannot be stored in plaintext form and storage must ensure security controls consistent with the security specifications for the device.

Subscribers may 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.

6.2.5 Private Key Archival

Subscriber private keys are not archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys are generated by and in a cryptographic module when one is used. If a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

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

The RA generating private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens.

6.2.8 Method of Activating Private Key

Subscribers must use the process subscribed in the CP (if any) to activate private keys.

6.2.9 Method of Deactivating Private Keys

Cryptographic modules that have been activated are not available to unauthorized access. After use, the cryptographic modules are deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. When deactivated, private keys are kept in encrypted form only.

6.2.10 Method of Destroying Private Key

RA personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers may destroy their private signature keys when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

6.3 Other Aspects of Key Pair Management

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Subscriber public keys and private keys have a maximu m designated usage period of twenty years. The RA does not issue subscriber certificates that extend beyond the expiration date of their own certificate and public keys.

Participants must cease all use of their key pairs after their usage periods have expired.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

RA personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. RA personnel are encouraged to create non-dictionary, alphanumeric passwords with a minimum length.

6.4.2 Activation Data Protection

The RA and Subscriber activation PINs are only known by the holder of the token (if used). The holder shall protect the entry of activation data from disclosure.

6.4.3 Other Aspects of Activation Data

The RA will follow the requirements of the reference documents in section 1.6.3. To the extent activation data for their private keys are transmitted, Activation Data Participants protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent desktop computer or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network must be protected against access by unauthorized users.

6.6 Life Cycle Technical Controls

RA equipment (hardware and software) should be purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. Intended use of procured hardware and software is never indicated on order forms/paperwork.

For all cryptographic hardware a verifiable chain of custody is maintained through all life cycle stages including: equipment receipt, surrender and physical storage. All cryptographic hardware should be handled by trusted employees of the RA organization. All packages are inspected upon receipt for signs of tamper/neglect. Any tamper-evident package that is received in an unsealed condition is deemed compromised. Virus scanning software should be installed on all RA equipment. Scans are conducted on first use and periodically afterward

7. CERTIFICATE, CRL, AND OCSP PROFILES

DigiCert sets the appropriate certificate, CRL, and OCSP profiles. RAs are only permitted to provide verification for the profiles authorized by DigiCert.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency of Compliance Audit

The RA undergoes an annual compliance audit. Compliance audits are conducted in accordance with DigiCert Private PKI CP/CPS section 8, the requirements of applicable consortium, and per relevant legal contracts.

8.2 Identity/Qualifications of Reviewer

Where independence is required, the RA selects an auditor, subject to the qualifications described herein. That auditor demonstrate competence in the field of compliance audits, and is thoroughly familiar with this RPS and the reference documents in section 1.6.3. The auditor must be a certified information system auditor (CISA), or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

Audits performed by an independent third party audit firm are performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm also has demonstrated expertise in the performance of IT security and PKI compliance audits.

The qualified audit firm is bound by law, government regulation, or professional code of ethics and maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Auditor's Relationship to Audited Party

Independent auditors selected must be a private firm that is independent from the RA being audited, or it will be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. Compliance auditors should not have a conflict of interest that hinders their ability to perform auditing services. To insure independence and objectivity for independent audits, the compliance auditor may not have served the entity in developing or maintaining the entity's RA Facility or RPS.

8.4 Topics Covered by Compliance Audit

RAs must undergo the audits required by the applicable policy in annual increments. The purpose of the annual compliance audit shall be to verify that the RA has complied with all the mandatory requirements of the current versions applicable CP and CPS.

Part of the Compliance Audit verifies that the RA has in place a system to assure the quality of RA services that it provides and that it complies with the requirements of this RPS and the CP. All aspects of the RA operations are subject to compliance audit inspections.

The RA components may be audited fully or by using a representative sample. If the auditor uses a statistical sampling, all components, component managers and operators are considered in the sample and the samples are varied on an annual basis.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of the applicable CP, RPS, and/or the design, operation, or maintenance of the RA functions, the following actions are performed:

- The compliance auditor notes the discrepancy;
- The compliance auditor promptly notifies the responsible parties identified in Section 8.6 of thediscrepancy;
- The party responsible for correcting the discrepancy proposes a remedy, including expected time for completion, to the RA and CA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, DigiCert may decide to temporarily halt operation of the RA, revoke a certificate issued to the RA, or take other actions it deems

appropriate. The actions taken depend on risk associated with a deficiency, the requirements of the community, and the nature of the RA.

In the event the RA fails to develop a corrective action plan to be implemented in a timely manner, or if the report reveals exceptions or deficiencies that DigiCert reasonably believes poses an immediate threat to the security or integrity of DigiCert or relying parties:

- Whether revocation and compromise reporting are necessary;
- Be entitled to suspend services to the RA; and
- If necessary, may terminate such services where there is substantial risk to stakeholders.

8.6 Communication of Results

Following any Compliance Audit, DigiCert may provide the results and any identification of corrective measures to third parties. RAs are required to provide all audit results to DigiCert in a timely fashion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

Additionally, where necessary, the results are communicated as set forth in section 8.5 above.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The RA may charge Subscribers a fee for the issuance, management, and renewal of certificates.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

RAs should maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following Subscriber information must be kept confidential and private by the RA:

- Certificate Application records;
- CA application status, whether approved or disapproved;
- Transactional records (both full records and the audit trail of transactions);
- Audit trail records; and
- Audit reports (as applicable as stated in section 8 of this RPS).

9.3.2 Information not Within the Scope of Confidential Information

The RA acknowledge that Certificates, Certificate revocation and other status information and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under the DigiCert Private PKI CP/CPS are considered neither confidential nor private.

9.3.3 Responsibility to Protect Confidential Information

The RA receiving private information secures it from compromise and disclosure to third parties.

9.4 Privacy

9.4.1 Privacy Plan

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private. The RA will have a Privacy Plan to protect personally identifying information from unauthorized disclosure.

9.4.2 Information Treated as Private

All non-certificate information received from Subscribers is treated as confidential by the RA. The RA does not disclose or sell applicant names or other identifying information, and does not share such information, except in accordance with this RPS. Records of individual transactions may be released upon request of any Subscribers involved in the transaction, their legally recognized agents, or as required by law.

9.4.3 Information Not Deemed Private

Information included in Certificates is deemed pubic information and is not subject to protections outlined in section 9.4.2. Information in a certificate is not considered private or privacy act information.

9.4.4 Responsibility to Protect Private Information

The RA does not disclose confidential information to any third party unless required by law, government rule or regulation, or order of a court of competent jurisdiction. The RA does not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release.

9.4.5 Notice and Consent to Use Private Information

The RA is not required to provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations in section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

All disclosure is pursuant to the DigiCert Private PKI CP/CPS, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.5 Intellectual Property Rights

DigiCert retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers that are the respective Subjects of these Certificates.

This RPS is the personal property of the RA.

9.6 Representations and Warranties

This section sets forth obligations and defines specific responsibilities for the following parties participating in the PKI described in this RPS:

- Registration Authority (RA)

The parties are hereby notified of the following rules and obligations governing the respective rights and obligations of the parties among themselves. These rules and obligations are deemed to be agreed by the parties effective upon publication of this RPS.

Additional obligations are set forth in other provisions of this RPS.

9.6.2 RA Obligations

An RA who performs registration functions as described in this RPS complies with the stipulations of this RPS and the reference documents in section 1.6.3. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA conforms to the stipulations of this document, including:

- Performing identify verification of certificate applicants in accordance with Section 3.2.3;
- Maintaining its operations in conformance to the stipulations of the approved RPS;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate;
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
- Ensuring that obligations are imposed on Subscribers, and that Subscribers are informed of the consequences of not complying with those obligations; and
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representation and Warranties

Subscribers must sign an agreement containing the requirements the Subscriber shall meet including protection of their private keys and use of the certificates before being issued the certificates.

In addition, Subscribers warrant that:

- The Subscriber must abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates;
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- Subscriber's private keys are protected from unauthorized use or disclosure;
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
- All information supplied by the Subscriber and contained in the Certificate is true;
- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of the applicable policy and technical specification requirements, and this RPS;
- The Subscriber will promptly notify the RA upon suspicion of loss or compromise of their private key(s);
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise

In the case of the automated process for issuance of device certificates the above duties are carried out by the person responsible of the device. For smooth manufacturing process, the tasks above are not mandatory upon acceptance of every certificate.

9.6.5 Representations and Warranties of Other Participants

9.6.5.2 DigiCert Obligations

The DCPA:

- Maintains and approves this RPS;
- Reviews periodic compliance audits to ensure that RAs are operating in compliance with the RPS and communicates the results of the annual compliance audit reports as stipulated in section 8.6;
- Reviews name space control procedures to ensure that distinguished names are uniquely assigned; and,
- Notifies appropriate entities in the event of RA compromise or termination.

9.12 Amendments

9.12.1 Procedure for Amendment

The DCPA, prior to enactment, approves material amendments to this RPS.

9.12.2 Notification Mechanism and Period

Upon approval of an RPS modification by the DCPA, an updated version of this document is distributed to the RA for further distribution to the RA trusted personnel.