Registration Practices Statement

Grid Registration Authority
Approved December____ , 2011
Version 1.00

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the Grid Registration Practices Statement (GRPS). The GRPS outlines the procedures that the community members of the ________________Grid follow to comply with the DigiCert CP and CPS. If any inconsistency exists between this GRPS and the DigiCert CPS, the DigiCert CPS takes precedence.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the Grid Registration Practices Statement and was approved on _______________ by the DigiCert Policy Authority and ________ , herein referred to as the Grid Registration Authority (GRA).

1.3. PKI PARTICIPANTS

1.3.1. Certification Authority

DigiCert is a certification authority (CA) that issues high quality and highly trusted digital certificates in accordance with its CPS. As a CA, DigiCert performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

1.3.2. Registration Authority and RA Operator

GRA is the Registration Authority (RA) responsible for the verification and issuance approval for certificates issued to Subscribers. The RA is contractually obligated to abide by DigiCert's CPS and any industry standards that are applicable to an RA's role in certificate issuance, management, and revocation. An RA's practices are regularly reviewed for sufficiency by DigiCert. While the GRA maintains primary responsibility for the procedural sufficiency of the RA operations, it has delegated responsibility for the administrative and technical operations of the RA functions to _____, acting as an RA Operator.

1.3.3. Subscribers

Subscribers are the members of the grid community serviced by the GRA and their associated employees, agents, and subcontractors who use DigiCert's certificates to conduct secure transactions and communications. Subscribers are not always the party identified in a certificate, such as in a device certificate, group certificate, or when certificates are issued to an organization's employees. 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 DigiCert for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a certificate and/or digital signature provided by the GRA. Relying parties must check the appropriate CRL or OCSP response prior to relying on information included in a certificate.

1.3.5. Other Participants

GRA Community members may be designated as "Trusted Agents". Trusted Agents are community members that are authorized by the GRA, GRA Operator, or DigiCert to gather documentation in relation to the issuance of a digital certificate.

1.4. CERTIFICATE USAGE

A *digital certificate* (or *certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1. Appropriate Certificate Uses

Subscribers and Relying Parties may use issued certificates for the purposes set forth in DigiCert's CPS.

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.

Certificates may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

1.5. PRACTICE STATEMENT ADMINISTRATION

1.5.1. Organization Administering the Document

This RPS is maintained by the GRA, which can be contacted at:

[Name of GRA]
____
____
____

DigiCert may be contacted at:

DigiCert Policy Authority
Suite 200 - Canopy Building II
355 South 520 West
Lindon, UT 84042 USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481

1.5.2. Contact Person

The contact person for operations under this RPS is the GRA Operator, which may be contacted at:

____
____
____

1.5.3. Person Determining RPS Suitability

The GRA and the DigiCert Certificate Policy Authority (DCPA) are jointly responsible for determining the suitability and applicability of this RPS.

1.5.4. RPS Approval Procedures

The GRA and the DCPA approve this RPS and any amendments. Amendments are made by either updating the entire RPS or by publishing an addendum.

1.6. DEFINITIONS AND ACRONYMS

“Affiliated Organization” means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a certificate.

“Applicant” means an entity applying for a certificate.

“Application Software Vendor” means a software developer whose software displays or uses DigiCert certificates and distributes DigiCert’s root certificates.

“Key Pair” means a Private Key and associated Public Key.

“OCSP Responder” means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

“Private Key” means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

“Public Key” means the key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

“Relying Party” means an entity that relies upon either the information contained within a certificate or a time-stamp token.

“Relying Party Agreement” means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert’s Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.

“Subscriber” means either entity identified as the subject in the certificate or the entity that is receiving DigiCert’s time-stamping services.

“Subscriber Agreement” means an agreement that governs the issuance and use of a certificate that the Applicant must read and accept before receiving a certificate.

Acronyms:

CA	Certificate Authority or Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
DCPA	DigiCert Policy Authority
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IGTF	International Grid Trust Federation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer

TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

As specified in the DigiCert CP and CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. Some certificates, including certificates for intranet use and Unified Communications Certificates, may contain entries in the subject alternative name extension that are not intended to be relied upon by the general public.

3.1.2. Need for Names to be Meaningful

As specified in the DigiCert CP and CPS.

3.1.3. Anonymity or Pseudonymity of Subscribers

As specified in the DigiCert CP and CPS.

3.1.4. Rules for Interpreting Various Name Forms

As specified in the DigiCert CP and CPS.

3.1.5. Uniqueness of Names

Each certificate contains a unique subject name and/or serial number.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers are contractually required to refrain from requesting certificates with content that infringes on the intellectual property rights of another entity.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method to Prove Possession of Private Key

A certificate Applicant must submit a CSR to establish that it holds the Private Key corresponding to the Public Key in the certificate request. A PKCS#10 format or Signed Public Key and Challenge (SPKAC) is recommended.

3.2.2. Authentication of Organization Identity

Organizational certificate applicants are required to include their name and address in the certificate application. The applicant's name and address are verified using a reliable third party database, a government databases, or through direct means of communication with the entity or jurisdiction responsible for the organization's creation or recognition.

If these sources do not sufficiently verify the name and address, then the applicant is verified using official company documentation that is submitted by the applicant, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other relevant documents.

The applicant's right to use the domain name in SSL Certificates is verified using DigiCert's domain validation system. If an entity other than the domain owner is requesting the certificate, then the domain holder must submit documentation authorizing the Applicant's request for a certificate. This document must be signed by the Registrant (e.g. a domain owner's authorized representative) or the Administrative Contact on the Domain Name Registrar record.

3.2.3. Authentication of Individual Identity

The GRA, GRA Operator, or Trusted Agent obtains and submits the following documentation:

Certificate	Validation
SSL Server Certificates and Object Signing Certificates (issued to an individual)	1. A legible copy of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). This information is cross-checked with reliable data sources. 2. (if necessary) An additional form of identification from the applicant, such as recent utility bills, financial account statements, credit card, college/university ID credential, or equivalent document type. 3. Confirmation of applicant's ability to receive communication by telephone, postal mail/courier, or fax. GRA may also verify the applicant by obtaining a witnessed and signed declaration of identity. The signing must be witnessed by a GRA representative, a Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Device Sponsors	See section 3.2.3.3
Level 1 Client Certificates - Personal (email certificates) (Equivalent to NIST 800-63/Kantara Level 1 and FBCA CP Rudimentary)	Email verification of applicant's control of the email address or website listed in the certificate. For corporate email certificates, confirmation from the organization's human resources department of the employee's current employment or agency status.
Level 1 Client Certificates - Enterprise (Equivalent to NIST 800-63/Kantara Level 1, FBCA CP Rudimentary and Citizen & Commerce Class Common CP (C4) Assurance Level-2.16.840.1.101.3.2.1.14.2)	1. In-person appearance before GRA representative or Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: a. the ability to place or receive calls from a given number; or b. the ability to obtain mail sent to a known physical address. 3. Using an ongoing business relationship with the RA or the Trusted Agent or a partner company (e.g., a financial institution, airline, employer, or retail company). The following information is considered proof of a business relationship: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receive phone calls at a phone number used in previous business transactions.

IGTF Certificates	1. In-person proofing before the RA, a notary, or a Trusted Agent with presentment of a government-issued photo ID that is examined for authenticity and validity. If GRA uses a notary, then the notary must send the documentation to the GRA Operator directly using a method that ensures secure delivery. 2. Remotely verifying the Applicant's name, date of birth, and current address or telephone number using a government-issued photo ID and one additional form of ID such as another government-issued ID, an employee or student ID card number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the Applicant's residence. GRA may verify the Applicant's address or telephone number by sending mail to the address or making a call to the telephone number. If a telephone call is made, then GRA or its representative must record the Applicant's voice. GRA must request additional information if necessary to ensure a unique identity. 3. If GRA has a current, ongoing relationship with the Applicant, then GRA may rely on the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.

3.2.3.1. Authentication for Role-based Client Certificates

GRA does not issue role-based client certificates.

3.2.3.2. Authentication for Group Client Certificates

GRA does not issue group client certificates.

3.2.3.3. Authentication of Devices with Human Sponsors

GRA may verify the information necessary for the issuance of Client and Federated Device Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, GRA collects device information from the human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment public keys,
3. Equipment authorizations and attributes (if any are to be included in the certificate), and
4. Contact information.

If the certificate's sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive certificates. The GRA Operator contacts sponsors annually using verified information to ensure that the device is still under the sponsor's control or responsibility. Sponsors shall notify GRA if the equipment is no longer in use or no longer requires a certificate. GRA shall verify each registration in accordance with the requested certificate type.

3.2.4. Non-verified Subscriber Information

IGTF, Object Signing, and Federated Device certificates only include verified information.

3.2.5. Validation of Authority

GRA shall verify the authority of the individual requesting a certificate on behalf of an organization as follows:

Certificate	Verification
SSL Server and Federated Device Certificates	DigiCert verifies the authenticity of the certificate request using a means of communication obtained from a reliable third party source.
Object Signing Certificates	The contact information and authority of the certificate requester is confirmed with an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources).
Level 1 Client Certificates - Personal (email certificates)	The individual's control over the email address listed in the certificate is verified through email.
Level 1 Client Certificates - Enterprise (email certificates)	The authorization of the organization named in the certificate is verified with a person who has technical or administrative control over the domain name.
IGTF Certificates	The authorization of the organization named in the certificate is verified with a person who has technical or administrative control over the domain name. The organization is required to request revocation of the certificate when that affiliation ends

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

As specified in the DigiCert CP and CPS.

3.3.2. Identification and Authentication for Re-key After Revocation

DigiCert will not rekey a certificate if it was revoked for any reason other than a renewal or update action. These Subscribers are re-verified using the initial registration process.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The GRA Operator must authenticate all revocation requests. The GRA Operator may authenticate revocation requests using the Certificate's Public Key, even if the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

GRA may accept a certificate application from either the applicant or an individual authorized to request certificates on behalf of the Applicant. For certificates that include a domain name, the Domain Name Registrar record maintained by the domain registrar presumptively indicates who has authority over the domain. If a certificate request is submitted by an agent of the domain owner, the agent must also submit a document that authorizes Subscriber's use of the domain.

GRA may not provide certificates to an entity that is on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

4.1.2. Enrollment Process and Responsibilities

The GRA Operator shall require each applicant to submit a certificate request and application information prior to issuing the certificate. The GRA Operator must implement a system that protects all communication from an applicant from modification.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

The applicant is verified in accordance with Section 3.2. After verification is complete, the verifier must evaluate the corpus of information and decides whether or not to issue the certificate.

The GRA Operator shall ensure that all communication between DigiCert and GRA regarding certificate issuance or changes in the status of a certificate are made using secure and auditable methods. The GRA Operator shall protect all sensitive information obtained from the Applicant and securely exchange this information with DigiCert in a confidential and tamper-evident manner that is protected from unauthorized access. The GRA Operator must track the exchange using an auditable chain of custody.

4.2.2. Approval or Rejection of Certificate Applications

The GRA Operator shall reject any certificate application that is not sufficiently verified. The GRA Operator shall also reject a certificate application if issuing the certificate could damage or diminish DigiCert's reputation or business.

If some or all of the documentation used to support the application is in a language other than English, an employee of the GRA Operator skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence. GRA may also rely on a translation of the relevant portions of the documentation by a qualified translator.

If the certificate application is not rejected and is successfully validated, the GRA Operator will approve the certificate application, upload all of the information used to verify the applicant to a server controlled by DigiCert, and issue the certificate. Rejected applicants may re-apply. Subscribers are required to check the data listed in the certificate for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

GRA shall confirm certificate application information and requests issuance of the digital certificate within a reasonable time frame, usually within two days after receiving all necessary details and documents from the Applicant.

4.3. CERTIFICATE ISSUANCE

4.3.1. Actions during Certificate Issuance

The GRA Operator shall verify the source of a certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate.

4.3.2. Notification to Subscriber of Issuance of Certificate

The GRA Operator may deliver certificates in any secure manner within a reasonable time after issuance.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's issuance.

4.4.2. Publication of the Certificate

End-entity certificates are published by delivering them to the Subscriber.

4.4.3. Notification of Certificate Issuance to Other Entities

As specified in the DigiCert CP and CPS.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers are contractually required 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 Private Keys only as specified in the key usage extension.

4.5.2. Relying Party Public Key and Certificate Usage

As specified in the DigiCert CP and CPS.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

The GRA Operator may authorize the renewal of a certificate if:

1. the associated public key has not reached the end of its validity period,
2. the Subscriber name and attributes are unchanged,
3. the associated private key remains un compromised, and
4. re-verification of the Subscriber's identity is not required under Section 3.3.1.

The GRA Operator shall make reasonable efforts to notify Subscribers via email of the imminent expiration of a digital certificate and may begin providing notice of pending expiration 60 days prior to the expiration date.

4.6.2. Who May Request Renewal

Only an authorized representative of a Subscriber may request renewal of the Subscriber's certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are the same as those used during the certificate's original issuance. GRA may not renew a certificate if any rechecked information cannot be verified. Identity information can be reused if location and Domain Name Registrar information have not changed. If the Subscriber's contact information and Private Key have not changed, the Subscriber may use the same CSR as was used for the previous certificate.

4.6.4. Notification of New Certificate Issuance to Subscriber

The GRA Operator shall deliver renewed certificates to Subscribers in a secure fashion.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's renewal.

4.6.6. Publication of the Renewal Certificate

Renewed certificates are published by delivering the certificate to the Subscriber.

4.6.7. Notification of Certificate Issuance to Other Entities

As specified in the DigiCert CP and CPS.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a certificate consists of creating a new certificate with a new public key and serial number while keeping the subject information the same. The new certificate may have a different validity period, key identifiers, CLR and OCSP distributions, and a different signing key. After re-keying a certificate, the Subscriber may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.7.2. Who May Request Certificate Rekey

The certificate subject may request certificate rekey.

4.7.3. Processing Certificate Rekey Requests

If the Subscriber's other contact information and Private Key have not changed, the Subscriber may use the previously provided CSR. Otherwise, the Subscriber must submit a new CSR. GRA may re-use existing verification information unless re-verification is required under section 3.3.1 or GRA believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

The GRA Operator shall notify the Subscriber within a reasonable time after the certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.7.6. Publication of the Issued Certificate

Rekeyed certificates are published by delivering them to Subscribers.

4.7.7. Notification of Certificate Issuance to Other Entities

As specified in the DigiCert CP and CPS.

4.8. CERTIFICATE MODIFICATION

As specified in the DigiCert CP and CPS.

4.8.1. Who May Request Certificate Modification

The GRA Operator or a Subscriber may request modification of a certificate.

4.8.2. Processing Certificate Modification Requests

Prior to requesting certificate modification, GRA shall verify any information that will change. GRA shall not request a modified certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.3. Notification of Certificate Modification to Subscriber

The GRA Operator shall notify the Subscriber within a reasonable time after the modified certificate issues.

4.8.4. Conduct Constituting Acceptance of a Modified Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.8.5. Publication of the Modified Certificate

Modified certificates are published by delivering them to Subscribers.

4.8.6. Notification of Certificate Modification to Other Entities

As specified in the DigiCert CP and CPS.

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, GRA shall verify the identity and authority of the entity requesting revocation. GRA must revoke a certificate if any of the following occur:

1. The Subscriber requested revocation of its certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised;
4. The Subscriber breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement;
5. The Subscriber's or GRA's obligations under the CP or CPS 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;
6. The certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
7. GRA received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. GRA's right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
9. A court or arbitrator revoked the Subscriber's right to use a name or mark listed in the certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
10. Any information appearing in the Certificate was or became inaccurate or misleading;
11. 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;
12. For code-signing certificates, the certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

GRA must also revoke a certificate if the binding between the subject and the subject's public key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2. Who Can Request Revocation

The Subscriber or another appropriately authorized party may request revocation of a certificate. GRA may require that the revocation request be made by either the organizational contact, billing contact or domain registrant.

GRA shall revoke a certificate if it receives sufficient evidence of compromise of loss of the private key. Entities other than the certificate subject may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report". All certificate revocation requests must include the identity of the entity requesting revocation and the reason for revocation.

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. After receiving a revocation request:

1. The GRA Operator shall log the identity of the entity making the request or problem report and the reason for requesting revocation and submit a copy of the request to DigiCert.
2. If applicable, GRA shall confirm the revocation request with a known administrator via out-of-band communication (e.g., telephone, fax, etc.). GRA must always revoke the certificate if the request is confirmed as originating from the Subscriber.
3. If the request originated from a third party, then GRA shall investigate the report within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of complaints/reports received about a particular certificate or website,
    c. the entity making the complaint (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.
4. If revocation is appropriate, the GRA Operator shall revoke the Certificate.

The GRA Operator shall maintain a continuous 24/7 ability to internally respond to any high priority complaints and problems. If appropriate, the GRA Operator may forward complaints to law enforcement.

4.9.4. Revocation Request Grace Period

As specified in the DigiCert CP and CPS.

4.9.5. Time within which RA Processes the Revocation Request

The GRA Operator shall process all certificate revocation requests within 18 hours after their receipt.

4.9.6. Revocation Checking Requirement for Relying Parties

As specified in the DigiCert CP and CPS.

4.9.7. CRL Issuance Frequency

CRLS are issued at least every 24 hours.

4.9.8. Maximum Latency for CRLs

As specified in the DigiCert CP and CPS.

4.9.9. On-line Revocation/Status Checking Availability

As specified in the DigiCert CP and CPS.

4.9.10. On-line Revocation Checking Requirements

As specified in the DigiCert CP and CPS.

4.9.11. Other Forms of Revocation Advertisements Available

As specified in the DigiCert CP and CPS.

4.9.12. Special Requirements Related to Key Compromise

As specified in the DigiCert CP and CPS.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder.

4.10.2. Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3. Optional Features

OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices

4.12.2. No stipulation.Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

The GRA Operator shall implement a security policy that is designed to detect, deter, and prevent unauthorized access to GRA's operations.

5.1.2. Physical Access

The GRA Operator shall protect its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering.

5.1.3. Power and Air Conditioning

As specified in the DigiCert CP and CPS.

5.1.4. Water Exposures

As specified in the DigiCert CP and CPS.

5.1.5. Fire Prevention and Protection
As specified in the DigiCert CP and CPS.

5.1.6. Media Storage
The GRA Operator shall protect GRA's media from accidental damage and unauthorized physical access.

5.1.7. Waste Disposal
The GRA Operator shall shred and destroy all out-dated or unnecessary copies of printed sensitive information before disposal. The GRA Operator shall zeroize all electronic media used in the RA operations using programs that meet the U.S. Department of Defense requirements.

5.1.8. Off-site Backup
The GRA Operator shall maintain at least one full backup and make regular backup copies of any information necessary to recover from a system failure.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles
Personnel acting in trusted roles include GRA's system administration personnel and personnel involved with identity vetting and the issuance and revocation of certificates. GRA shall distribute the functions and duties performed by persons in trusted roles so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. GRA shall ensure that all personnel in trusted roles are free from conflicts of interest that might prejudice the impartiality of GRA's operations. GRA shall maintain a list of personnel appointed to trusted roles and review this list annually.

5.2.2. Number of Persons Required per Task
As specified in the DigiCert CP and CPS.

5.2.3. Identification and Authentication for each Role
GRA shall require all personnel to authenticate themselves to GRA's systems before they are allowed access to the system.

5.2.4. Roles Requiring Separation of Duties
Roles requiring a separation of duties include:

1. The verification of information in certificate applications,
2. The approval of certificate applications, and
3. The approval of revocation requests.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements
GRA's practices shall 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 GRA Operator shall verify the identity of each person appointed to a trusted role and perform a background check prior to allowing the person to act in a trusted role. The GRA Operator shall require each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee shall verify 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 checks must include employment history, education, character references, social security number, previous residences, driving records and criminal background. Background investigations are performed by a competent independent party that has the authority to perform background investigations. The GRA Operator shall perform checks of previous residences are over the past three years. All other checks are for the previous five years. The GRA Operator shall verify the highest education degree obtained regardless of the date awarded. The GRA Operator shall refresh background checks at least every ten years.

5.3.3. Training Requirements

The GRA Operator shall provide skills training to all personnel involved in PKI operations. The training relates to the person's job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by the GRA Operator,
3. authentication and verification policies and procedures,
4. disaster recovery and business continuity procedures,
5. common threats to the validation process, including phishing and other social engineering tactics, and
6. applicable industry and government guidelines.

The GRA Operator shall maintain records of who received training and what level of training was completed. The GRA Operator shall provide these records to DigiCert upon request. Validation personnel must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. The GRA Operator shall make all individuals acting in trusted roles aware of any changes to GRA's operations. If GRA's operations change, GRA must provide documented training to all personnel acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

As specified in the DigiCert CP and CPS.

5.3.6. Sanctions for Unauthorized Actions

GRA shall make any employee or agent that fails to comply with this RPS or the DigiCert CPS subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by DigiCert or GRA for unauthorized or inappropriate actions, GRA must immediately remove that person from the trusted role pending review.

5.3.7. Independent Contractor Requirements

GRA shall make its independent contractors who are assigned to perform trusted roles subject to the duties and requirements specified for such roles in this Section 5.3 and subject to the sanctions stated in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

GRA shall provide personnel in trusted roles the documentation necessary to perform their duties, including a copy of this RPS.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

GRA systems shall require identification and authentication at system logon using a unique user name and password. The GRA Operator shall enable all essential event auditing capabilities of its operations in order to record the events listed below. If an application cannot automatically record an event, the GRA Operator shall use a manual procedure to satisfy these requirements. For each event, the GRA Operator shall record 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. The GRA Operator shall make these event records available to DigiCert and DigiCert's auditors as proof of GRA's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by remote access to the RA systems
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL AND REJECTION
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
File manipulation (e.g., creation, renaming, moving)
All certificate compromise notification requests
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches

Auditable Event
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of the CPS or RPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

The GRA Operator shall periodically review the logs generated by GRA's systems, make system and file integrity checks, and conduct a vulnerability assessment. During these checks, the GRA Operator shall (1) check whether anyone has tampered with the log, (2) scan for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepare a written summary of the review. The GRA Operator shall investigate any anomalies or irregularities found in the logs. The GRA Operator shall make these logs available to DigiCert upon request.

5.4.3. Retention Period for Audit Log

The GRA Operator shall retain audit logs on-site until after they are reviewed.

5.4.4. Protection of Audit Log

GRA Operator personnel are required to keep all generated audit log information on their equipment until after it is copied by a system administrator. The GRA Operator shall configure its systems to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period.

5.4.5. Audit Log Backup Procedures

The GRA Operator shall make backup copies of its audit logs on a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes must begin on system startup and end at system shutdown. GRA shall promptly notify DigiCert if the integrity of the system or confidentiality of the information protected by a system is at risk.

5.4.7. Notification to Event-causing Subject

As specified in the DigiCert CP and CPS.

5.4.8. Vulnerability Assessments

GRA shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of its RA systems. GRA shall routinely assess the sufficiency of its risk control policies, procedures, information systems, technology, and other arrangements.

5.5. RECORDS ARCHIVAL

GRA shall comply with all record retention policies that apply by law. GRA shall include sufficient detail in all archived records to show that a certificate was issued in accordance with the CPS.

5.5.1. Types of Records Archived

GRA shall retain the following information in its archives:

1. RPS versions,
2. Contractual obligations and other agreements regarding certificates,
3. System and equipment configurations, modifications, and updates,
4. Certificate and revocation requests,
5. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2,
6. Any documentation related to the receipt or acceptance of a certificate or token,
7. Subscriber Agreements,
8. A record of certificate re-keys,
9. Data or applications necessary to verify an archive's contents,
10. Changes to GRA's audit parameters,
11. Attempts to delete or modify audit logs,
12. Access to Private Keys for key recovery purposes,
13. Export of Private Keys,
14. Approval or rejection of a certificate status change request,
15. Appointment of an individual to a trusted role,
16. Certificate compromise notifications,
17. Remedial action taken as a result of violations of physical security, and
18. Violations of the RPS or the CPS.

5.5.2. Retention Period for Archive

GRA shall retain archived data for at least 10.5 years.

5.5.3. Protection of Archive

GRA shall store archive records in a manner that prevents unauthorized modification, substitution, or destruction. GRA shall maintain any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If the GRA Operator needs to transfer any media to a different archive site or equipment, the GRA Operator shall maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives must occur in a secure manner.

5.5.4. Archive Backup Procedures

GRA shall create an archive disk of the data listed in section 5.5.1 annually and stores it in a secure off-site location for the duration of the 10.5-year retention period.

5.5.5. Requirements for Time-stamping of Records

The GRA Operator shall automatically time-stamp archived records with system time (non-cryptographic method) as they are created. The GRA Operator shall synchronize its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

GRA shall stamp and record information collected during the identity verification process, including IP addresses associated with applicant submissions and screen shots provided by verification information sources where applicable.

5.5.6. Archive Collection System (internal or external)

As specified in the DigiCert CP and CPS.

5.5.7. Procedures to Obtain and Verify Archive Information

As specified in the DigiCert CP and CPS.

5.6. KEY CHANGEOVER

Not applicable.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

The GRA Operator shall promptly notify DigiCert if a disaster causes GRA's operations to become inoperative.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

The GRA Operator shall reestablish operations as quickly as possible after a disaster or data corruption.

5.7.3. Entity Private Key Compromise Procedures

Not applicable.

5.7.4. Business Continuity Capabilities after a Disaster

The GRA Operator shall implement data backup and recovery procedures. The GRA Operator shall develop a Business Continuity Management Program (BCMP) that is reviewed, tested, and updated annually.

5.8. RA TERMINATION

Before GRA terminates RA activities, the GRA Operator shall:

1. Provide notice and information about the termination by sending notice by email to its customers and by posting such information on GRA's web site; and
2. Transfer all certificate responsibilities to DigiCert.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

Subscriber public keys must be generated in a secure manner that is appropriate for the certificate type.

6.1.2. Private Key Delivery to Subscriber

If GRA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. GRA may deliver keys electronically or on a hardware cryptographic module / SSCD. In all cases:

1. GRA may not retain a copy of the Subscriber's Private Key after delivery,
2. GRA must protect the private key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the private key(s), and
4. GRA must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
    b. For electronic delivery of private keys, encrypting key material using a cryptographic algorithm and key size at least as strong as the private key. GRA will deliver activation data using a separate secure channel.

GRA shall maintain a record of the Subscriber’s acknowledgement of receipt of the device containing the Subscriber’s Key Pair. GRA provides a copy of this record to DigiCert.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers generate key pairs and submit the Public Key to GRA in a CSR as part of the certificate request process. The Subscriber’s signature on the request is authenticated prior to issuing the certificate.

6.1.4. CA Public Key Delivery to Relying Parties

As specified in the DigiCert CP and CPS.

6.1.5. Key Sizes

Subscriber keys must be at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms, except for certificates issued to smart cards or other hardware devices that are incapable of accepting 2048-bit RSA certificates, then the key length must be at least 1024 bits for RSA and that the certificate expire on or before December 31, 2013. Any certificates expiring after 12/31/2030 must be at least 3072-bit for RSA and 256-bit for ECDSA.

Signatures on all certificates are generated using at least SHA-1. Federated Device Certificates require the use of the SHA-256 algorithm.

Subscribers may fulfill their requirements using TLS or another protocol that provides similar security, provided the protocol requires at least:

1. AES (128 bits) or equivalent for the symmetric key and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010, and
2. AES (128 bits) or equivalent for the symmetric key and at least 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

6.1.6. Public Key Parameters Generation and Quality Checking

As specified in the DigiCert CP and CPS.

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

Key usage bits and extended key usages are specified in the certificate profile for each type of certificate.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

IGTF Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect private keys. Cryptographic module requirements are shown in the table below.

Assurance Level	Subscriber	RA / RA Operator
Client Certificates	N/A	FIPS 140 Level 1 (Hardware or Software)
IGTF	FIPS 140 Level 1 (Hardware or Software)	FIPS 140 Level 1 (Hardware or Software)

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

As specified in the DigiCert CP and CPS.

6.2.3. Private Key Escrow

Subscribers may not escrow their private signature keys or dual use keys. GRA may provide escrow services for Subscriber Private Keys used for encryption in order to provide key recovery as described in section 4.12.1.

6.2.4. Private Key Backup

GRA may provide backup services for (1) Level 1 subscriber private signature keys provided that the backup copies are held in the Subscriber's control and (2) subscriber key management keys. Backup keys are stored with security controls that are consistent with the protection provided by the Subscriber's cryptographic module. Backed up keys can never be stored in a plain text form outside of the cryptographic module.

6.2.5. Private Key Archival

GRA may not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module.

6.2.7. Private Key Storage on Cryptographic Module

As specified in the DigiCert CP and CPS.

6.2.8. Method of Activating Private Keys

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their private keys.

6.2.9. Method of Deactivating Private Keys

As specified in the DigiCert CP and CPS.

6.2.10. Method of Destroying Private Keys

Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed.

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

As specified in the DigiCert CP and CPS.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

As specified in the DigiCert CP and CPS.

6.4. ACTIVATION DATA

As specified in the DigiCert CP and CPS.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

The GRA Operator shall secure GRA's systems and authenticate and protect communications between its systems and trusted roles. GRA's servers and support-and-vetting workstations must run on trustworthy systems that are configured and hardened using industry best practices. The

GRA Operator shall scan all of GRA's systems for malicious code and shall protect such systems at all times against spyware and viruses.

GRA's systems, including any remote workstations, must be configured to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

6.5.2. Computer Security Rating

As specified in the DigiCert CP and CPS.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

The GRA Operator shall control and monitor the acquisition and development of GRA's RA systems. The GRA Operator shall only install software on RA systems that is necessary to GRA's operation.

The GRA Operator shall select vendors based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. The GRA Operator shall have all hardware and software shipped under standard conditions to ensure delivery of the component directly to a trusted employee who installs the equipment without opportunity for tampering.

Software developed in-house or by consultants using standard software development methodologies were developed using a formal, documented, development methodology in a controlled environment. Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

The GRA Operator shall scan all hardware and software essential to GRA's operations for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

The GRA Operator has mechanisms in place to control and monitor the security-related configurations of its RA systems, including change control data entries that are processed, logged and tracked for any security-related changes. When loading software onto a RA system, the GRA Operator verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

As specified in the DigiCert CP and CPS.

6.7. NETWORK SECURITY CONTROLS

The GRA Operator shall document and control the configuration of its systems, including any upgrades or modifications made. The GRA Operator shall protect its systems with firewall(s) and shall only use internal IP addresses. The GRA Operator shall configure its firewalls and boundary control devices to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of its RA services.

The GRA Operator shall block all ports and protocols and open only necessary ports to enable RA functions. All RA equipment is configured with a minimum number of services and all unused network ports and services are disabled. The GRA Operator shall allow DigiCert to review its network configuration upon request.

6.8. TIME-STAMPING

The system time on computers operating the RA process must be updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to the real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body.

7. CERTIFICATE, CRL, AND OCSP PROFILES

As specified in the DigiCert CP and CPS.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2. Certificate Extensions

As specified in the DigiCert CP and CPS. IGTF certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

7.1.3. Algorithm Object Identifiers

As specified in the DigiCert CP and CPS.

7.1.4. Name Forms

Each certificate includes a unique serial number that is never reused.

7.1.5. Name Constraints

As specified in the DigiCert CP and CPS.

7.1.6. Certificate Policy Object Identifier

The OIDs used by GRA are set forth in DigiCert's Certificate Profiles document.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

Certificates may include a brief statement about the limitations of liability and other terms associated with the use of a certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

As specified in the DigiCert CP and CPS.

7.2. CRL PROFILE

7.2.1. Version number(s)

As specified in the DigiCert CP and CPS.

7.2.2. CRL and CRL Entry Extensions

As specified in the DigiCert CP and CPS.

7.3. OCSP PROFILE

As specified in the DigiCert CP and CPS.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

DigiCert electronically audits GRA's issuance systems and procedures. DigiCert may audit GRA's compliance with the CPS at any time.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

DigiCert personnel are responsible for auditing GRA's compliance with this RPS.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

GRA is a RA of DigiCert.

8.4. TOPICS COVERED BY ASSESSMENT

The audit covers GRA's systems and validation process.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports any material noncompliance with applicable law, this RPS, the CPS, the CP, or any other contractual obligations related to GRA's services (to the extent such information is audited), then (1) DigiCert will document the discrepancy, (2) DigiCert will promptly notify the GRA Operator, and (3) the GRA Operator will develop a plan to cure the noncompliance.

8.6. COMMUNICATION OF RESULTS

As specified in the DigiCert CP and CPS.

8.7. SELF-AUDITS

The GRA Operator shall perform regular internal audits to ensure compliance with this RPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

As specified in the DigiCert CP and CPS.

9.2. FINANCIAL RESPONSIBILITY

As specified in the DigiCert CP and CPS.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The GRA Operator shall protect the following as confidential information using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access to GRA's systems;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by GRA as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2. Information Not Within the Scope of Confidential Information

Information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

The GRA Operator shall contractually obligate its employees, agents, and contractors to protect confidential information. The GRA Operator shall ensure that employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

The GRA Operator follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when required by law or when requested by the subject of the personal information. The GRA Operator will disclose information related to the issuance or use of a certificate to DigiCert upon request.

9.4.2. Information Treated as Private

The GRA Operator shall treat all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. The GRA Operator shall protect private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

The GRA Operator shall handle personal information in strict confidence and shall meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

Personal information provided during the application or identity verification process is considered private information provided that the information is not included in a Certificate. Each party shall only use private information after obtaining the subject's express written consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

GRA may disclose private information, without notice, when required to do so by law or regulation.

9.4.7. Other Information Disclosure Circumstances

As specified in the DigiCert CP and CPS.

9.5. INTELLECTUAL PROPERTY RIGHTS

Certificate and revocation information are the exclusive property of DigiCert. DigiCert does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the DigiCert Private Keys are the property of DigiCert.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

DigiCert’s offers the warranties described in its CPS.

9.6.2. RA Representations and Warranties

GRA represents that:

1. GRA’s certificate issuance and management services conform to the DigiCert CP and CPS,

2. Information provided by the GRA Operator does not contain any false or misleading information,
3. Translations performed by the GRA Operator are an accurate translation of the original information, and
4. All certificates requested by the GRA Operator meet the requirements of the DigiCert CPS.

9.6.3. Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to represent to DigiCert, Application Software Vendors, and Relying Parties that, for each certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with the GRA Operator,
3. Confirm the accuracy of the certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify the GRA Operator if (i) any information that was submitted to the GRA Operator or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, the CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate and not using code signing certificates to sign malicious code or any code that is downloaded without a user's consent,
7. Abide by the Subscriber Agreement and the CPS when requesting or using a Certificate, and
8. Promptly cease using the certificate and related Private Key after the certificate's expiration.

9.6.4. Relying Party Representations and Warranties

As specified in the DigiCert CP and CPS.

9.6.5. Representations and Warranties of Other Participants

As specified in the DigiCert CP and CPS.

9.7. DISCLAIMERS OF WARRANTIES

DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.8. LIMITATIONS OF LIABILITY

The limitations of liability related to DigiCert's certificates are set forth in DigiCert's CPS and are incorporated into the Subscriber Agreements.

9.9. INDEMNITIES

9.9.1. Indemnification by RA

GRA's indemnification obligations are set forth in a contract between GRA and DigiCert.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber is contractually obligated to indemnify DigiCert and any cross-signed entities, and their respective partners, directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, the CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the certificate or Private Key.

9.9.3. Indemnification by Relying Parties

As specified in the DigiCert CP and CPS.

9.10. TERM AND TERMINATION

9.10.1. Term

This RPS and any amendments to the RPS are effective when approved by DigiCert and the GRA Operator and remain in effect until replaced with a newer version.

9.10.2. Termination

This RPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

The GRA Operator shall communicate the conditions and effect of this RPS's termination in a manner mutually agreed to by DigiCert and the GRA Operator. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Notices requirements are set forth in the agreement between the parties.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This RPS is reviewed annually. Amendments are made by mutual agreement between DigiCert and the GRA Operator.

9.12.2. Notification Mechanism and Period

Notice of amendments is not provided to any third party.

9.12.3. Circumstances under which OID Must Be Changed

As specified in the DigiCert CP and CPS.

9.13. DISPUTE RESOLUTION PROVISIONS

As specified in the DigiCert CP and CPS.

9.14. GOVERNING LAW

The laws of the state of Utah govern the interpretation, construction, and enforcement of this RPS and all proceedings related to DigiCert's products and services, including tort claims, without regard to any conflicts of law principles. The courts of the state of Utah have non-exclusive venue and jurisdiction over any proceedings related to the RPS or any DigiCert product or service.

9.15. COMPLIANCE WITH APPLICABLE LAW

As specified in the DigiCert CP and CPS.

9.16. MISCELLANEOUS PROVISIONS

As specified in the DigiCert CP and CPS.

9.17. OTHER PROVISIONS

As specified in the DigiCert CP and CPS.