Registration Practices Statement

Open Science Grid
Approved ___________ , 2012
Version 1.00

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

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

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the OSG Registration Practices Statement and was approved on _______________ by the DigiCert Policy Authority and OSG.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

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 Authorities

OSG is the Registration Authority (RA) responsible for the verification and issuance of certificates issued under DigiCert's grid-only arc. Indiana University (the OSG Operator) operates the RA on behalf of the community and is responsible for ensuring OSG's compliance with this RPS and the CPS. OSG is obligated to abide by DigiCert's CPS and any industry standards that are applicable to OSG's role in certificate issuance, management, and revocation.

1.3.3. Subscribers

Subscribers are the members of OSG 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 OSG. Relying parties must check the appropriate CRL or OCSP response prior to relying on information included in a certificate.

1.3.5. Other Participants

OSG member organizations are designated as "Trusted Agents". Trusted Agents are authorized by OSG and DigiCert to gather documentation in relation to the issuance of a digital certificate. Trusted Agents act as OSG's representative for the purpose of facilitating certificate issuance to the Trusted Agent's employees, contractors, agents, and affiliated entities. An administrator designated by the Trusted Agent administrator is responsible for ensuring the Trusted Agent's compliance with this RPS and the CPS.

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

Certificates issued under this RPS may be used only for authentication and digital signatures within the grid network and to create proxy certificates. This grid-only limitation is enforced through the certificate chain (end-entity certificates are chained to a root certificate that is not embedded in browser software).

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 are not appropriate (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 OSG Operator, which can be contacted at:

Indiana University
____
____
____

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

Indiana University
____
____
____

1.5.3. Person Determining RPS Suitability

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

1.5.4. RPS Approval Procedures

The OSG Operator 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

"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.

“Subscriber” means either entity identified as the subject in a certificate.

“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
DCPA	DigiCert Policy Authority
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

Root certificates, revocation data, CP, and CPS information is published in DigiCert’s publicly available repositories on DigiCert’s website. Root certificates and CRLs are available 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year. The RPS is provided by the OSG Operator to Trusted Agents and other interested participants upon receipt of a written request.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The DigiCert repository is available on DigiCert's website at www.digicert-grid.com.

2.3. TIME OR FREQUENCY OF PUBLICATION

CA certificates are published within a reasonable time after issuance. CRLs for end-user certificates are issued at least once per day. CRLs include a monotonically increasing sequence number. New CRLs may be published prior to the expiration of the current CRL. Updated CPS documents are published after their approval by the DigiCert policy authority.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Grid certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards.

3.1.2. Need for Names to be Meaningful

Grid certificates use unique distinguished names to identify both the subject and issuer of the certificate.

3.1.3. Anonymity or Pseudonymity of Subscribers

OSG does not provide anonymous or pseudonymous certificates.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

Each certificate issued under this RPS contains a unique subject name. Unique subject names for individuals are created by appending a user ID that is unique to the applicant to the applicant's name. Trusted Agents are not permitted to request issuance of a certificate with a distinguished name of an existing certificate if the identity information does not adequately prove that the subjects of both the old and new certificate are the same entity. Device certificates include the FQDN of the host.

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

An 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

The Applicant's information is verified by having the appropriate Trusted Agent verify that (i) the certificate information is correct, (ii) the applicant is authorized to request the certificate, and (iii) the applicant is authorized to use any listed domain name listed in the certificate.

3.2.3. Authentication of Individual Identity

Either a Trusted Agent must attest that the Applicant is personally known to the Trusted Agent or OSG or a Trusted Agent must obtain a copy of a photo-identification or similar document of the applicant during a face-to-face meeting. If an identification document is used, sufficient information about the applicant's identity must be recorded and archived in order to ensure that identity of the individual can be confirmed at a later date. If the applicant is personally known, an attestation of the Trusted Agent must be recorded and archived.

3.2.4. Non-verified Subscriber Information

OSG certificates include only verified information.

3.2.5. Validation of Authority

OSG verifies that the Trusted Agent is authorized to request and approve certificates on behalf of the Trusted Agent's organization. Trusted Agents are responsible for designating which individuals in their organization are authorized obtain host certificates and are required to confirm this authority prior to requesting a certificate. The Trusted Agent authorizing issuance of a device certificate must retain contact information for each device's registered owner and request revocation if the device's sponsor's authorization to use the FQDN in the certificate or the device is terminated.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

OSG certificates have a validity period of 13 months. OSG may rekey/renew certificates prior to their expiration date for additional 13 month periods up to a maximum of five years. OSG or a Trusted Agent revalidates the certificate information at least once every five years.

3.3.2. Identification and Authentication for Re-key After Revocation

OSG may not rekey a certificate if it was revoked for any reason other than for renewal or certificate modification. OSG must re-verify the information in these certificates using the initial registration process.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The OSG Operator must authenticate all revocation requests. The OSG 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

OSG may accept certificate applications from Trusted Agents and other authorized organizations and individuals. OSG 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

Trusted Agents verify the identity of a certificate applicant prior to authorizing the issuance of a certificate. Trusted Agents and the OSG Operator use protected communication to interact with DigiCert's certificate issuing systems.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

The applicant is verified in accordance with Section 3.2. The OSG Operator shall protect all sensitive information obtained from the Applicant.

4.2.2. Approval or Rejection of Certificate Applications

The OSG Operator shall reject any certificate application that it considers inadequately verified. The OSG Operator shall also reject a certificate application if issuing the certificate could damage or diminish DigiCert's reputation or business. Rejected applicants may re-apply. Subscribers are required to check the data listed in the certificate for accuracy prior to using the certificate.

If some or all of the documentation used to support the application is in a language other than English, an employee of the OSG 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. OSG may also rely on a translation of the relevant portions of the documentation by a qualified translator.

4.2.3. Time to Process Certificate Applications

OSG confirms certificate application information and requests issuance of the digital certificate within a reasonable time frame after receiving all necessary details and documents from the Applicant.

4.3. CERTIFICATE ISSUANCE

4.3.1. Actions during Certificate Issuance

The OSG 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 OSG 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. A certificate may be delivered using any reasonably secure method to delivery.

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 OSG Operator may renew 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.

4.6.2. Who May Request Renewal

Trusted Agents or an authorized representative of a Subscriber may request renewal of the Subscriber's certificates.

4.6.3. Processing Certificate Renewal Requests

No additional verification is required if the certificate subject information has not changed and less than five years have passed since the certificate's information was verified. A Trusted Agent must represent that the renewal request is authorized.

4.6.4. Notification of New Certificate Issuance to Subscriber

The OSG Operator shall use contact information provided by the Subscriber to notify the Subscriber of the certificate's issuance.

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

Trusted Agents and OSG may receive notice of a certificate renewal.

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, OSG 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

Trusted Agents or an authorized representative of a Subscriber may request certificate rekey.

4.7.3. Processing Certificate Rekey Requests

No additional verification is required if less than five years have passed since the certificate's information was verified. A Trusted Agent must represent that the rekey request is authorized.

4.7.4. Notification of Certificate Rekey to Subscriber

The OSG Operator shall use contact information provided by the Subscriber to notify the Subscriber of the certificate's issuance.

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

Trusted Agents and OSG may receive notice of a certificate rekey.

4.8. CERTIFICATE MODIFICATION

4.8.1. Who May Request Certificate Modification

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

4.8.2. Processing Certificate Modification Requests

Prior to requesting certificate modification, OSG shall verify any information that will change. OSG 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 OSG Operator shall use contact information provided by the Subscriber to notify the Subscriber of the certificate's issuance.

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

Trusted Agents and OSG may receive notice of a certificate modification.

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, OSG shall verify the identity and authority of the entity requesting revocation. OSG 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 OSG'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. OSG received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. OSG'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. Any information appearing in the Certificate was or became inaccurate or misleading; or
10. 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.

OSG 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

Subscribers are required to request revocation within one working day after detecting a loss or compromise of the Private Key or if the certificate data is no longer valid. OSG may accept revocation requests from entities other than the subscriber. OSG may require entities to verify their identity prior to accepting a revocation request. Entities submitting certificate revocation requests should list their identity and explain the reason for requesting revocation.

4.9.3. Procedure for Revocation Request

OSG logs each revocation request and submits a copy of the request to DigiCert. OSG will revoke a certificate if the revocation request originated from the subscriber. If a third party requested revocation, OSG will investigate the request before revoking the certificate. Factors considered in revoking a certificate include the nature of the problem, the number of complaints received, and the entity making the request.

If appropriate, OSG may forward complaints to law enforcement.

4.9.4. Revocation Request Grace Period

OSG Certificates do not have a revocation grace period.

4.9.5. Time within which RA Processes the Revocation Request

The OSG Operator processes certificate revocation requests in a timely manner, but no later than one working day.

4.9.6. Revocation Checking Requirement for Relying Parties

As specified in the DigiCert CP and CPS.

4.9.7. CRL Issuance Frequency

CRLS for OSG-provided certificates 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
OSG does not provide key escrow services.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices
As specified in the DigiCert CP and CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction
The OSG Operator shall implement a security policy that is designed to detect, deter, and prevent unauthorized access to OSG's operations.

5.1.2. Physical Access
The OSG 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 OSG Operator shall protect OSG's media from accidental damage and unauthorized physical access.

5.1.7. Waste Disposal

The OSG Operator shall shred and destroy all out-dated or unnecessary copies of printed sensitive information before disposal. The OSG 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 OSG 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 OSG's system administration personnel and personnel involved with identity vetting and the issuance and revocation of certificates. OSG 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 RA operations. OSG shall ensure that all personnel in trusted roles are free from conflicts of interest that might prejudice the impartiality of OSG's operations.

5.2.2. Number of Persons Required per Task

No stipulation.

5.2.3. Identification and Authentication for each Role

OSG shall require users accessing RA systems to enter a valid password prior to using the system.

5.2.4. Roles Requiring Separation of Duties

No stipulation.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

OSG'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

No stipulation.

5.3.3. Training Requirements

Trusted Agents and/or OSG shall provide periodic 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 OSG,
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.

OSG shall maintain records of who received training and what level of training was completed. OSG shall provide these records to DigiCert upon request.

5.3.4. Retraining Frequency and Requirements

No stipulation.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

No stipulation.

5.3.7. Independent Contractor Requirements

No stipulation.

5.3.8. Documentation Supplied to Personnel

OSG 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

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

Auditable Event
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
Successful and unsuccessful attempts to assume a role in OSG's systems
The value of maximum number of authentication attempts to OSG's systems is changed
Maximum number of authentication attempts to OSG system's occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
All security-relevant messages that are received by remote access to OSG's systems
Verification activities
Logon attempts to DigiCert's API through OSG's interface
All certificate compromise notification requests
Known or suspected violations of physical security related to OSG's RA systems
Firewall and router activities
Software error conditions related to OSG's RA activities
Network attacks (suspected or confirmed) related to OSG's RA activities
Violations of the CPS or RPS

5.4.2. Frequency of Processing Log

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

5.4.3. Retention Period for Audit Log

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

5.4.4. Protection of Audit Log

OSG Operator systems used in the RA function must retain all generated audit log information until after it is copied by a system administrator. The OSG Operator shall configure its RA 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 OSG 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 on RA systems must begin on system startup and end at system shutdown. OSG 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

No stipulation.

5.4.8. Vulnerability Assessments

OSG 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. OSG shall routinely assess the sufficiency of its risk control policies, procedures, information systems, technology, and other arrangements.

5.5. RECORDS ARCHIVAL

OSG shall comply with all record retention policies that apply by law. OSG 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

Trusted Agents must retain the following information and provide copies of such information upon request to DigiCert:

1. Contractual obligations and other agreements regarding certificates, including agreements with applicants specifying the terms of certificate use,
2. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2,

OSG retains the following information and provides such information to DigiCert upon request:

1. Certificate and revocation requests,
2. Changes to OSG's audit processes,
3. Attempts to delete or modify OSG's audit logs,
4. Approval or rejection of a certificate status change request,
5. Certificate compromise notifications,
6. Remedial action taken as a result of violations of physical security, and

7. Violations of the RPS or the CPS by OSG, a Trusted Agent, or Subscriber.

5.5.2. Retention Period for Archive

OSG shall retain archived data for as long as there are valid certificates whose issuance was based on the archived data.

5.5.3. Protection of Archive

OSG shall store archive records in a manner that prevents unauthorized modification, substitution, or destruction. OSG 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 OSG Operator needs to transfer any media to a different archive site or equipment, the OSG 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

OSG shall create an archive disk of the data listed in section 5.5.1 annually and store it securely for the duration of the retention period.

5.5.5. Requirements for Time-stamping of Records

The OSG Operator shall automatically time-stamp archived records with system time (non-cryptographic method) as they are created. The OSG 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.

OSG 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)

The OSG operator is responsible for collecting and archiving information related to OSG's RA operations.

5.5.7. Procedures to Obtain and Verify Archive Information

The OSG Operator may establish procedures that allow parties to obtain archived information. The OSG Operator shall make archived information available to DigiCert after receiving a written request from DigiCert.

5.6. KEY CHANGEOVER

Not applicable.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

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

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

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

5.8. RA TERMINATION

Before OSG terminates RA activities, the OSG Operator shall:

1. Provide notice and information about the termination by sending notice by email to its customers and by posting such information on OSG's web site; and
2. Either request revocation of the issued certificates or transfer the 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 OSG generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. OSG may deliver keys electronically or on a hardware cryptographic module / SSCD. In all cases:

1. OSG may not retain a copy of the Subscriber's Private Key after delivery,
2. OSG 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. OSG 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. OSG will deliver activation data using a separate secure channel.

OSG shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. OSG 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 OSG 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

As specified in the DigiCert CP and CPS.

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

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. Private keys for grid certificates must be generated using trustworthy cryptographic hardware or software (for example, a FIPS 140-2 Level 1 or higher cryptographic module).

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

Signing keys are security protected when not in use and may only be accessed by actions of multiple trusted DigiCert personnel.

6.2.3. Private Key Escrow

OSG does not provide key escrow services.

6.2.4. Private Key Backup

OSG does not backup keys.

6.2.5. Private Key Archival

OSG does 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

DigiCert's keys are generated and stored inside DigiCert's cryptographic modules.

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

Subscribers should deactivate their Private Keys when not in use.

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

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

OSG certificates have a maximum validity period of 13 months. 2048-bit Private Keys generated on hardware can be used for 60 months. 1024-bit Private Keys generated on hardware can be used for 36 months. Certificates using Private Keys generated using software must be rekeyed every 13 months. Subscribers generating keys using a software cryptographic module must protect the Private Key using a strong password (at least 12 characters long and following current best practices).

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 OSG Operator shall secure OSG's systems and authenticate and protect communications between its systems and trusted roles. OSG's servers and support-and-vetting workstations must run on trustworthy systems that are configured and hardened using industry best practices. The OSG Operator shall scan all of OSG's RA systems for malicious code and shall protect such systems at all times against spyware and viruses.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

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

The OSG 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 OSG 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.

6.6.2. Security Management Controls

The OSG 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 OSG 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

No stipulation.

6.7. NETWORK SECURITY CONTROLS

The OSG Operator shall document and control the configuration of its systems, including any upgrades or modifications made. The OSG 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 OSG 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 OSG 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

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. Certificates issued under this RPS 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 or user ID that is never reused.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

The OIDs used by OSG 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

No stipulation.

7.2. CRL PROFILE

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 audits OSG's compliance with this RPS and the CPS on an annual basis. Audits of OSG's validation process are conducted using a randomly selected sample of certificates. OSG audits its Trusted Agent's validation process on an annual basis using a randomly selected sample of certificates.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

DigiCert personnel are responsible for auditing OSG's compliance with this RPS. OSG personnel are responsible for auditing Trusted Agents.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

OSG is a RA of DigiCert. Trusted Agents are members of OSG's organizational group.

8.4. TOPICS COVERED BY ASSESSMENT

Audits of OSG cover OSG's systems and validation process. Audits may also include a Trusted Agent's procedure for performing the certificate validation required under this RPS.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If a DigiCert audit discovers any material noncompliance with applicable law, this RPS, the CPS, the CP, or any other contractual obligations related to OSG's services (to the extent such information is audited), then (1) DigiCert will document the discrepancy, (2) DigiCert will promptly notify the OSG Operator, and (3) the OSG Operator will develop a plan to cure the noncompliance. If OSG's audit of a Trusted Agent discovers any material noncompliance by a Trusted Agent with this RPS, then OSG will (1) document the discrepancy, (2) promptly notify DigiCert, and (3) develop a plan to cure the non-compliance.

8.6. COMMUNICATION OF RESULTS

The results of an audit are reported to DigiCert's policy authority any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7. SELF-AUDITS

The OSG Operator shall perform regular self audits to ensure that OSG and the Trusted Agents are in compliance with this RPS. To the extent possible, the OSG Operator may conduct these audits electronically by requesting a copy of the documentation relied on in issuing the certificate.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

OSG may charge fees for certificate services.

9.2. FINANCIAL RESPONSIBILITY

OSG's certificates are not publicly trusted and are not covered by an insurance policy.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

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

1. Information and data used to access DigiCert's systems;
2. Business continuity, incident response, contingency, and disaster recovery plans;
3. Information held by OSG as private information in accordance with Section 9.4;
4. Audit logs and archive records; and
5. 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 OSG Operator shall contractually obligate its employees, agents, and contractors to protect confidential information. The OSG 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 OSG 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 OSG 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 OSG 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 OSG Operator shall protect private information using appropriate safeguards and a reasonable degree of care, including encrypting private information when in transit to and from OSG's RA systems.

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 OSG Operator shall handle personal information in strict confidence and shall meet the requirements of all applicable laws 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

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

9.4.7. Other Information Disclosure Circumstances

No stipulation.

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

OSG represents that:

1. OSG's certificate issuance and management services conform to the DigiCert CP and CPS,

2. Information provided by the OSG Operator does not contain any false or misleading information,
3. Translations performed by the OSG Operator are an accurate translation of the original information, and
4. All certificates requested by the OSG 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 OSG Operator,
3. Confirm the accuracy of the certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify the OSG Operator if (i) any information that was submitted to the OSG 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,
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

The products and services provided under this RPS may be modified or discontinued as set forth in a contract between OSG and DigiCert .

9.8. LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM DIGICERT'S NEGLIGENCE OR (II) FRAUD COMMITTED BY DIGICERT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A DIGICERT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF DIGICERT RELATED TO SUCH USE.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether DigiCert failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective. The disclaimers and limitations on liabilities in this RPS are fundamental terms to the use of DigiCert's certificates and services.

9.9. INDEMNITIES

9.9.1. Indemnification by OSG

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

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber is contractually obligated (via an online click-through agreement) 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 OSG 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 OSG Operator shall communicate the conditions and effect of this RPS's termination in a manner mutually agreed to by DigiCert and the OSG 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

Notice 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 OSG Operator.

9.12.2. Notification Mechanism and Period

Notices of amendments are not provided to any third party.

9.12.3. Circumstances under which OID Must Be Changed

DigiCert is responsible for determining when an OID must be changed.

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.