CILogon Open Science Grid Certification Authority Certificate Policy and Certification Practice Statement (CP/CPS)

December 05, 2017

Version 3
1.3.6.1.4.1.34998.1.6.3

https://opensciencegrid.github.io/security/OSGCertificateService/

Contents

1. INTRODUCTION

1.1 Overview

This document is a combined Certificate Policy and Certification Practice Statement for the CILogon Open Science Grid Certification Authority. It is structured according to RFC 3647.

The CA issues end entity certificates to Open Science Grid members. Identification and authentication of certificate applicants is performed by the Open Science Grid Registration Authority, which is operated by the OSG Operations Center at Indiana University.

Subscribers obtain a certificate from the CA according to the following process. The subscriber visits OIM website to make a request. The Open Science Grid Information Management (OIM) system provides the graphical user interface for the CA services. The OIM collects the following from the subscriber: the name of the subscriber, the contact information (phone, email and address), a password, the Virtual Organization (VO) membership, and his/her consent to the CILogon OSG CA Certificate Subscriber Agreement. Once the request is submitted, the OIM identifies the Registration Authority Agent assigned to the VO specified in the request, and the RA Agent verifies the identity of the user and his/her affiliation with the VO. If the verification is successful, the CILogon OSG CA issues a signed X.509 certificate containing the subject distinguished name to the subscriber.

The CA is subject to accreditation by the International Grid Trust Federation (via The Americas Grid Policy Management Authority under the Authentication Profile for Classic X.509 Public Key Certification Authorities with Secured Infrastructures. This profile applies to traditional X.509 Public Key Certification Authorities (traditional PKI CAs) that issue long-term credentials to end-entities, who will themselves possess and control their key pair and their activation data. The CA acts as an independent trusted third party for both subscribers and relying parties within the infrastructure. The CA uses a long-term signing key, which is stored in a secure manner.

1.2 Document name and identification

Name: CILogon Open Science Grid Certification Authority Certificate Policy and Practice Statement
Version: 3
Date: December 05, 2017
ASN.1 object identifier: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1) CILogon Project (34998) Certificate Policies (1) CILogon OSG CA (6) Version (3)

Revision history:

1. October 12, 2015: Initial version.
2. March 30, 2016: Added E-mail Protection to X509v3 Extended Key Usage on End entity personal certificates.
3. December 05, 2016: Modified contact person and updated links to public repositories.

1.3 PKI participants

1.3.1 Certification authorities

The CA issues end entity certificates. It does not issue certificates to any subordinate CAs.

1.3.2 Registration authorities

Identification and authentication of certificate applicants is performed by the Open Science Grid (OSG). OSG Operations Center (GOC) at Indiana University operates the OSG Registration Authority and is responsible for verification and issuance of the certificates. OSG is comprised of a number of Virtual Organizations (VOs) that are members of OSG. For each VO, the OSG Registration Authority assigns a Registration Authority Agent (RA Agent), who is responsible for validating the certificate requests. To assist the RA Agents, each VO also identifies a list of Sponsors, who help with verifying the subscribers' requests. The sponsors are located at institutions that are active participants in their VOs. Sponsors can typically verify a subscriber's identity face-face because they are both located at the same institution. When a face-face meeting is not possible, identity verification is conducted as explained in Section 3.2. The RA Agents are ultimately responsible for granting or rejecting a request and they manage the process for their VOs.

For host/service certificate requests, a special kind of RA Agent, called a Grid Admin, verifies that the machine and the domain identified in the certificate request belongs to the requestor. Each VO registers their institutions and their fully qualified domain names with the OSG RA. Each registered institution is assigned a group of Grid Admins who can verify whether a host/service

certificate request within their domain should be granted or not.

1.3.3 Subscribers

The subscribers of the CA are Open Science Grid users and administrators.

1.3.4 Relying parties

The relying parties of the CA are the Open Science Grid sites, the International Grid Trust Federation relying party members, and any other recipient of a certificate issued by the CA who acts in reliance on that certificate and/or any digital signatures verified using that certificate.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

The CA issues certificates for use in authenticating to cyber-infrastructure.

1.4.2 Prohibited certificate uses

The CA makes no prohibitions on the use of the certificates it issues.

1.5 Policy administration

1.5.1 Organization administering the document

This policy is administered by the OSG Security Officer (osg-security-team@opensciencegrid.org).

The CA is subject to accreditation by the International Grid Trust Federation (via The Americas Grid Policy Management Authority) under the Authentication Profile for Classic X.509 Public Key Certification Authorities with Secured Infrastructures. All policy changes are subject to IGTF/TAGPMA review and approval.

1.5.2 Contact person

Susan Sons
Center for Applied Cybersecurity Research - Indiana University
2719 E. 10th Street, Suite 231

Bloomington, IN 47408
sesons@iu.edu
Office: 812-856-2949
Fax: 812-856-7400

For inquiries and fault reporting, contact help@opensciencegrid.org.

1.5.3 Person determining CPS suitability for the policy

This combined CP/CPS is administered by the OSG Security Officer (osg-security-team@opensciencegrid.org), which determines its suitability. All versions of this policy are submitted to the IGTF/TAGPMA for review and approval prior to operation.

1.5.4 CPS approval procedures

The OSG Security Officer approves CP/CPS changes. TAGPMA CP/CPS approval procedures are specified in the TAGPMA Charter.

1.6 Definitions and acronyms

This document uses terms as defined in Section 2 of RFC 3647.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The CA publishes information regarding its practices, certificates, contact information, etc., at OSG Certificate Service

The root CA certificate is delivered to relying parties according to Section 6.1.4.

2.2 Publication of certification information

The CA publishes certification information at the following locations:

https://opensciencegrid.github.io/security/OSGCertificateService/	web page of the CA for general information
CILogon OSG CP/CPS V3	the current version of this policy
CILogon OSG CA PEM	certificate

CILogon OSG CA DER	self-signed DER-formatted CA certificate
http://crl.cilogon.org/cilogon-osg.r0	PEM-formatted CRL
http://crl.cilogon.org/cilogon-osg.crl	DER-formatted CRL

The CA web page contains (in addition to the above):

- all versions of this CP/CPS document under which valid certificates have been issued
- an official contact email address (help@opensciencegrid.org) for inquiries and fault reporting
- a postal contact address

2.3 Time or frequency of publication

CRLs will be published immediately after a certificate has been revoked as well as on a daily basis. The CRL's This Update field will indicate the issue date of the CRL, and the Next Update field will be set to 30 days in the future, to indicate a 30 day validity period for the CRL.

CA certificates will be published on the CA web page and also submitted to external distributions/repositories (see Section 6.1.4) in advance of their use in operation. Under normal circumstances, the CA will not begin operation with a new CA certificate until that certificate has been distributed/published in all locations specified in Section 6.1.4 for at least one week (allowing time for relying parties to update their installations of CA certificates).

Any modifications to this policy must be published at least two weeks prior to their taking effect.

2.4 Access controls on repositories

Read access to repositories via HTTP is unrestricted. Repositories are publicly available for read access.

Write access to repositories is restricted to CA operators.

The OSG Security Officer grants the International Grid Trust Federation and its PMAs the right of unlimited redistribution of this information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The subject and issuer names are X.500 distinguished names. All relative distinguished name components are encoded as PrintableString and are compliant with RFC 4630 and GFD.125.

The issuer name for all certificates is:

/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon OSG CA 1

The CA updates the issuer CN in case of key changeover (Section 5.6), so that each "CILogon OSG CA #" for a given numeric "#" value unambiguously corresponds to a unique CA keypair and self-signed CA certificate. Updates to the issuer name constitute a change to this document (Section 9.12).

The subject name template for personal certificates is:

/DC=org/DC=opensciencegrid/O=Open Science Grid/OU=People/CN=*Given Name Surname disambiguator*

The subject name template for host/service certificates is:

/DC=org/DC=opensciencegrid/O=Open Science Grid/OU=Services/CN=*FQDN*

For example:

- DC=org, DC=opensciencegrid, O=Open Science Grid, OU=People, CN=Jane Doe 456
- DC=org, DC=opensciencegrid, O=Open Science Grid, OU=Services, CN=test.example.edu
- DC=org, DC=opensciencegrid, O=Open Science Grid, OU=Services, CN=rsv/test.example.edu

The subject alternative name (subjectAltName) extension contains an Internet mail address of type rfc822Name (for example: jbasney@cilogon.org). For host/service certificates, this is the email address of the person who requested the certificate.

3.1.2 Need for names to be meaningful

The commonName (CN) component contains the subscriber's name, as vetted, authenticated, and asserted by the OSG Registration Authority. The subject alternative name contains the subscriber's contact email address as registered with and asserted by the OSG Registration Authority.

3.1.3 Anonymity or pseudonymity of subscribers

The CA does not support anonymity or pseudonymity of subscribers.

3.1.4 Rules for interpreting various name forms

Subject and issuer names are X.500 distinguished names and should be interpreted according to RFC 4514, RFC 4630, and GFD.125. Internet mail addresses in subject alternative names are rfc822Names and should be interpreted according to RFC 2822.

3.1.5 Uniqueness of names

Any single subject distinguished name in a certificate is linked with one and only one entity for the lifetime of the CA. The CA assigns a unique numeric identifier to each subscriber, which is the subscriber's OIM account number. Each subscriber is given a unique OIM account upon requesting a certificate from OSG and the account number is linked with the subscriber's Common Name in the subject distinguished name. The OIM ID is not rotated and is not re-assigned to another subscriber. Device certificates are distinguished by the FQDN of the host.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

In the case the subscriber presents a public key for certification, the CA requires a certificate request that is digitally signed by the private key associated with the public key in the request. The key pair generation is described in Section 6.1

3.2.2 Authentication of organization identity

Not Applicable.

3.2.3 Authentication of individual identity

Any one of the methods listed below can be used to authenticate an individual:

- Existing Relationship. If the subscriber is personally known to a Registration Authority Agent (RA Agent) or a Sponsor associated with the subscriber's Virtual Organization, RA Agent or the Sponsor may use this authentication method. The RA Agent or the Sponsor must verify that the request is indeed coming from the subscriber. This can be done by a face-face meeting, or through an email address or the phone

number of the subscriber that is known to RA Agent or Sponsor before the identity vetting process. An attestation of the RA Agent or the Sponsor must be recorded and archived.

- In-Person Proofing. An RA Agent or a Sponsor must obtain a copy of a government-issued 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.

- Remote Proofing. If no RA Agent or Sponsor knows the subscriber personally and cannot meet face-face with the subscriber, the following methods can be used to authenticate the request.
    - Name, e-mail address and telephone number available from a publicly accessible directory of the institution where the subscriber is affiliated.
    - Unsigned e-mail from third parties known to the RA staff person attesting to the validity of the request
    - Information about the subscriber posted on institutional web sites, such as description of a research group on a university web site, or an institutional organization chart.

3.2.4 Non-verified subscriber information

The CA does not collect any non-verified subscriber information.

3.2.5 Validation of authority

OSG verifies that the Registration Authority Agents and Grid Admins are authorized to request and approve certificates on behalf of their Virtual Organizations. The Grid Admins are responsible for designating which individuals in their organizations are authorized to obtain host certificates and are required to confirm this authority prior to requesting a certificate. The subscribers must use their personal certificates in order to be authenticated during their host/service certificate request. Every VO registers a list of domain names owned by the VO and the list of Grid Admins assigned to each domain with the OSG RA. The Grid Admins for a particular domain has knowledge of who can operate services within their domain on behalf of their VOs. The Grid Admins 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.

3.2.6 Criteria for interoperation

The CA interoperates with other members of the International Grid Trust Federation (IGTF) according to standards such as RFC 5280 and GFD.125.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

End entity certificates have a validity period of 13 months. The CA may rekey/renew personal certificates prior to their expiration date for additional 13-month periods up to a maximum of five years. The OSG RA revalidates the certificate information at least once every five years. While making a re-key request, the subscriber is authenticated by using his/her unexpired certificate. If the certificate is already expired, the OSG RA will authenticate the request either as explained in Section 3.2 or by using the subscriber's contact information stored at OIM during the initial enrollment process.

The host/service certificates cannot be renewed or re-keyed, and a new request must be made. Each host/service certificate request must be authenticated by the requestor's personal certificate and must be verified by the Grid Admin as described in Section 4.1.2.

3.3.2 Identification and authentication for re-key after revocation

The CA may not rekey a certificate if it was revoked for any reason other than for re-key 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

OSG Registration Authority authenticates all revocation requests by using the certificate's public key, even if the associated Private Key is compromised. If the subscriber cannot use his/her certificate for authentication, the RA Agent authenticates the person by using the contact information stored in his/her OIM account. If the revocation request comes from a third party, the RA Agent authenticates the requestor either by the requestor's certificate or by the requestor's contact information in OIM. If neither is available, The RA Agent authenticates the third party according to the Section 3.2.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any person who is a member of a Virtual Organization that is an official member of OSG can submit a certificate application.

4.1.2 Enrollment process and responsibilities

Subscribers make a certificate request on the Open Science Grid Information Management (OIM) website, which is hosted at https://oim.grid.iu.edu/oim/certificaterequestuser. During the enrollment process, the OIM system creates an account for the user and collects the following information:

- Full Name,
- Phone,
- Email,
- City, State, Zipcode, and Country
- Profile, a few sentences to introduce themselves to the OSG community, the work they do and the role they play
- Virtual Organization of which they are a member
- Consent to CILogon OSG CA Certificate Subscriber Agreement
- A password to protect their private key

The subscriber sends this information over a TLS-protected channel to the OIM system. Once the certificate request is processed, the subscriber is notified via his/her email address provided above. If the request is denied, the subscriber can make another attempt remedying the issues causing the rejection. If the request is granted, the subscriber proceeds with requesting the issuance of the certificate. During the certificate issuance, the subscriber must supply the password chosen at the enrollment process. This step is an authentication layer verifying that the person issuing the certificate is indeed the same person who made the request. The OIM system generates the certificate signing request and have the CA sign it. Finally, the subscriber downloads the certificate and the private key in a PKCS12 file format and decrypts the private key with the same password supplied earlier.

For host/service certificates, each VO registers with OIM the list of their institutions and their fully qualified domain names, where the VO has computing resources. The VO manager specifies a group of Grid Admins for each domain and delegates the responsibility of managing certificate requests

to the Grid Admins. Grid Admins are located at the institutions that they manage. When a subscriber makes a host certificate request, he or she must present his/her personal certificate for authentication. The Grid Admins has knowledge of who can operate services within their domain for their VO. In case a Grid Admin does not recognize the requestor's need to operate services, the VO manager makes the final decision. Since Grid Admins are located at the same institution as the subscribers, they usually know the subscriber personally or meet with them in person.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Subscribers are authenticated as described in Section 3.2 and Section 4.1.2.

4.2.2 Approval or rejection of certificate applications

The OSG Registration Authority rejects any certificate application that it considers inadequately verified or missing required information. In particular, the subscriber must provide the information listed in Section 4.1.2 during the enrollment process. The OSG RA rejects any request that is coming from a subscriber who is not a member of a Virtual Organization in OSG.

4.2.3 Time to process certificate applications

The OSG RA confirms the certificate application information and makes a decision over the application as soon as receiving all necessary details and documents from the Applicant with the aim to complete within two business days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon approval of a certificate application and the subscriber's request for issuance, the CA assigns an X.500 distinguished name to the subscriber based on the information provided during the enrollment process and issues a signed X.509 certificate containing the subscriber's public key and subject distinguished name.

In order for CA to issue the certificate, the subscriber must first explicitly request the issuance of the certificate. Once a certificate request is approved by the OSG RA, the subscriber is notified of the decision via the OIM system.

After the notification, the subscriber visits the OIM, authenticates with his chosen password set during the enrollment period, and explicitly requests issuance of his/her certificate. Only then a CSR is generated by the OIM system and sent to the CA, which results in issuance of the actual certificate. It takes only a minute or so from the time the subscriber makes the issuance request until the CA issues the certificate. The subscriber remains in the same OIM session until he/she receives and downloads his/her certificate. As a result, there is no need to notify the subscriber when the certificate is issued. The subscriber understands that she/he needs to maintain its OIM session and is shown a message to wait for his/her certificate on the OIM website.

There is no direct communication between the OSG RA and the CA; all communication is handled by the OIM system. When RA approves the certificate request, he/she updates the status of the request in the OIM. When the subscriber explicitly requests issuance of the certificate, the OIM system makes an API request to the CA.

The communication between the RA Agents and the Sponsors are recorded in an OIM ticket. The contents of OIM tickets are publicly available; however, only authorized RA Agents and Sponsors can modify ticket contents either by using their email accounts or X509 certificates. The ticketing service runs on https. Likewise, OIM system runs on https and only allows authorized RA Agents and Sponsors with X509 certificates to make changes to the system. When the CA issues the certificate, the status in OIM as well as the ticket opened for this request is updated with this information. OIM tickets are archived indefinitely by the system and used during our annual audits to verify the RA Agents and Sponsors conduct.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Once a certificate application is approved, the OSG RA notifies the user through his/her contact information supplied during the initial enrollment process. The notification is done via the OIM ticketing system. If the request is granted, the subscriber visits the OIM website and starts a session. During the session, the subscriber must provide his/her password chosen during the enrollment process and must explicitly request the issuance of the certificate. Only after the subscriber's explicit request for issuance, the CA issues the certificate as described in Section 4.3.1 Since the certificate is automatically issued after the subscriber's request for issuance, there is no need for an additional notification to the user. The OIM updates the status of the OIM ticket and records the fact that a certificate has been issued in OIM ticketing system.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Certificate acceptance by the applicant is assumed. To reject an issued certificate, the subscriber should submit a revocation request according to Section 4.9.

4.4.2 Publication of the certificate by the CA

The CA does not publish end entity certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA does not notify any other entities of certificate issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers must protect their private keys according to the IGTF Guidelines on Private Key Protection.

Subscribers must request revocation as soon as possible (within one business day) if (1) the private key corresponding to the certificate is (suspected or known to be) lost or compromised or (2) if the data in the certificate is no longer valid. (See Section 4.9.)

The CA informs subscribers of these responsibilities on a web page they view when submitting certificate requests.

4.5.2 Relying party public key and certificate usage

Relying parties should rely on certificates consistent with applicable certificate content (e.g., key usage field), successfully perform public key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate (see Section 4.9), and not presume any authorization of a certificate subject based solely on possession of a certificate or its corresponding private key.

4.6 Certificate renewal

Certificate renewal is not supported. Subscribers must generate a new key pair for every certificate request.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Certificate re-key is supported. Subscribers can request re-keying for up to 5 years without having to verify their identities see Section 4.7.3.

4.7.1 Circumstance for certificate re-key

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.

4.7.2 Who may request certification of a new public key

Any subscriber can request certification of a new public key.

4.7.3 Processing certificate re-keying requests

No additional verification is required if less than five years have passed since the certificate's information was verified. The subscriber is authenticated by using his/her existing certificate. If subscriber's existing certificate is already expired, the subscriber may be authenticated according to Section 3.3.1

4.7.4 Notification of new certificate issuance to subscriber

The issuance process is identical to the process described in Section 4.3. The certificate issuance is triggered by the subscriber's request and is completed within a minute or so within the same OIM session. The subscriber creates an OIM session to request a renewal and is expected to stay in the same session until the new certificate is issued. As a result, there is no need for a separate notification for the subscriber. The OIM system creates a ticket for the application and records the actions taken during the request.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Certificate acceptance by the applicant is assumed. To reject an issued certificate, the subscriber should submit a revocation request according to Section 4.9.

4.7.6 Publication of the re-keyed certificate by the CA

The CA does not publish end entity certificates.

4.7.7 Notification of certificate issuance by the CA to other entities

The CA does not notify any other entities of the certificate issuance.

4.8 Certificate modification

Certificate modification is not supported. Instead, subscribers should submit a new certificate application according to Section 4.1.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The CA will revoke certificates in any of the following circumstances:

- The subscriber requests the revocation.
- The private key is suspected or reported to be lost or compromised.
- The initial identity validation for obtaining the certificate is determined to not comply with Section 3.2.
- The information in the certificate is believed to be or has become inaccurate.
- The certificate is reported to no longer be needed or the subscriber's affiliation with his/her VO and OSG has ended.
- OSG received a lawful and binding order from a government or regulatory body to revoke the certificate.
- The certificate was not issued in accordance with the CP, CPS, or applicable industry standards.
- 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)
- The Subscriber breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement.

4.9.2 Who can request revocation

Any participants can request revocation. Revocation requests will be authenticated according to Section 3.4.

4.9.3 Procedure for revocation request

Revocation requests may be submitted by email to help@opensciencegrid.org. OSG logs each revocation request. 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.

4.9.4 Revocation request grace period

Revocation requests should be submitted within one business day of the occurrence of any of the circumstances for revocation in Section 4.9.1.

4.9.5 Time within which CA must process the revocation request

The CA processes revocation requests within one working day of the request being received.

4.9.6 Revocation checking requirement for relying parties

Relying parties should consult the CRL in order to check the status of certificates on which they wish to rely.

4.9.7 CRL issuance frequency (if applicable)

A new CRL is issued daily and also when a certificate is revoked.

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency between the generation of CRLs and posting of the CRLs to the repository is one hour.

4.9.9 On-line revocation/status checking availability

Aside from the published CRL, no on-line revocation/status checking is provided.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re-key compromise

No stipulation.

4.9.13 Circumstances for suspension

Suspension of certificates is not supported.

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

The CA publishes the current CRL in DER format at http://crl.cilogon.org/cilogon-osg.crl with Content-Type: application/pkix-crl according to RFC 5280.

4.10.2 Service availability

The CA will endeavor to provide uninterrupted availability of the CRL service. Any significant availability disruptions will be announced by email to igtf-general@gridpma.org and also on the CA website.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A subscriber may end subscription to the CA services by requesting revocation (Section 4.9) of all certificates issued to the subscriber or by allowing all certificates issued to the subscriber to expire without requesting any new certificates.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

The CA does not support private key escrow and recovery.

4.12.2 Session key encapsulation and recovery policy and practices

The CA does not support session key encapsulation and recovery.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

CA equipment is located in NCSA's machine room in the National Petascale Computing Facility (NPCF) on the University of Illinois at Urbana-Champaign campus at 1725 South Oak Street in Champaign, Illinois (USA).

CA equipment is also located in Oak Ridge National Lab (ORNL) Building 5100, Oak Ridge, TN 37831-6173.

5.1.2 Physical access

CA equipment at NCSA is located in a locked rack inside the NCSA machine room. The machine room is locked at all times, requires keycard authentication for access, and is monitored by video camera. Only University of Illinois staff, approved by NCSA, are authorized to enter the machine room. The key to the rack is kept in the NCSA key safe, access to which is logged.

CA equipment at ORNL is located in a restricted, badge-access machine room, while ORNL campus requires a valid badge or visitor pass to be on-site. The machine room is locked at all times, requires keycard authentication for access and has 24x7 security monitoring for intrusion.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

CA system backups are archived weekly to a secondary storage facility in the NCSA Building on the University of Illinois at Urbana-Champaign campus at 1205 West Clark Street in Urbana, Illinois. The NCSA Building is approximately 3 miles away from NPCF, where the CA is located.

5.2 Procedural controls

5.2.1 Trusted roles

CA operators are responsible for the administration of all CA systems.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

CA operators authenticate by individual password or private key. When any person leaves the role of CA operator, his or her access to CA systems will be immediately revoked (i.e., system accounts removed or disabled).

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All CA operators are full-time university/lab employees.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

All CA operators are required to read and abide by all CA policy and operational documentation (Section 5.3.8). Current CA operators will train and mentor new CA operators.

5.3.4 Retraining frequency and requirements

All CA operators are required to review all CA policy and operational documents at least once per year.

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

The CA supplies policy and operational documentation to personnel including operators, RAs, Sponsors, and support staff. The RA Agents go through a training process before appointed as Agents and they refresh their training annually.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The CA logs and archives the following items:

- Certificate requests
- Certificate issuance
- Certificate revocations
- Issued CRLs
- Attempted and successful accesses to CA systems and reboots of those systems
- Actions taken during the initial identity vetting process to verify a subscriber's identity, such as phone numbers, emails, government-issued identities.

5.4.2 Frequency of processing log

The CA archives audit logs according to Section 5.1.8.

5.4.3 Retention period for audit log

The CA maintains audit logs for at least three years.

5.4.4 Protection of audit log

Only CA operators can view audit logs.

5.4.5 Audit log backup procedures

The CA archives audit logs according to Section 5.1.8.

5.4.6 Audit collection system (internal vs. external)

The audit collection system is internal to the CA.

5.4.7 Notification to event-causing subject

The subject who caused an audit event to occur is not notified of the specific audit action.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The CA archives all audit data (see Section 5.1.8 and Section 5.4).

5.5.2 Retention period for archive

The CA maintains archives for at least three years.

5.5.3 Protection of archive

No stipulation.

5.5.4 Archive backup procedures

See Section 5.1.8.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The maximum lifetime of the CA's public key is 20 years. The CA must not sign certificates with validity dates beyond the CA public key's maximum lifetime. Instead, the CA must re-key or cease operation (Section 5.8) in advance of reaching the maximum lifetime of the public key. The CA will also re-key in cases where the security of the current key is weakened, due to security incident, significant change in personnel, policy, or operations, or changes in recommended key length or algorithm.

The key changeover procedure is as follows. The CA generates a new key pair and delivers it to relying parties according to Section 6.1. The CA delivers the new key pair in a new self-signed CA certificate, with a new issuer name (Section 3.1.1). The CA amends this document according to Section 9.12, with the new issuer name and Policy OID, along with any other policy and/or procedure changes for the new key pair. In an emergency, the CA may begin operation under the new CA key pair immediately, but in non-emergency cases, the CA should perform the changeover in an orderly manner, providing sufficient time for relying parties to obtain and install the new self-signed CA certificate.

The procedures to provide a new public key to the CA's users following a re-key by the CA are the same as the procedure for providing the current key (Section 2.1). The new public key is not certified in a certificate signed using the old key (i.e., the CA signs only end entity certificates and not CA certificates).

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

CA operators will coordinate incident response and compromise handling with:

- University of Illinois incident response teams (NCSA)
- Open Science Grid incident response team
- International Grid Trust Federation (IGTF) incident response teams (i.e., the IGTF Risk Assessment Team)

In the event of a significant security incident, the CA will re-key (Section 5.6).

5.7.2 Computing resources, software, and/or data are corrupted

If computing resources, software, and/or data are corrupted or suspected to

be corrupted, CA operators will re-establish a secure environment with the assistance of incident response teams.

5.7.3 Entity private key compromise procedures

In the event of a CA private key compromise, the CA will revoke all certificates signed by that key, re-establish a secure environment, re-key (Section 5.6), and advise subscribers to re-apply (Section 4.1), in coordination with relying parties and incident response teams.

5.7.4 Business continuity capabilities after a disaster

CA operators maintain business continuity plans and capabilities including multi-site operations (at NCSA and ORNL), offsite backups (Section 5.1.8), and vendor support contracts for prompt replacement of CA hardware, including replacement of hardware security modules.

5.8 CA or RA termination

In the event that it is necessary for the CA to cease operation, the CA will develop a termination plan in consultation with participants that minimizes disruption to the extent possible. Archival CA records will be maintained by the University of Illinois in accordance with the stated retention period (Section 5.5.2).

RA appointments are renewed annually. If an RA Agent needs to be terminated before the end of his/her term, his/her RA Agent privileges in the OIM system will be deleted, effectively preventing him/her acting as an Agent.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA operators generate CA private keys using trustworthy cryptographic software, on an offline computer dedicated for this purpose, using a fresh operating system installation from known good media. After generating a new key pair, the CA operator imports it into the cryptographic modules (Section 6.2.6) and writes an encrypted backup to offline media (Section 6.2.4). CA operators record for audit purposes the time/date, location, personnel involved, computer, software, and operating system used, and details about the key pair created and cryptographic modules.

End entity private keys are generated and protected according to the IGTF

Guidelines on Private Key Protection.

The subscribers either generate the key pair themselves or have the OIM system generate one for them.

For the command-line client tools, the private key is generated by the subscriber either by explicitly generating a certificate signing request file on local disk or by having the command line client tools generate a CSR file. In both cases, the private key is stored on the subscriber's local disk and is never sent to any other parties. The command-line clients send the CSR file to the CA.

For the OIM interface that provides the web-based user interface, the OIM server generates the key pair by using the bouncycastle library. The key is stored only in memory during the OIM session, and it is never stored on disk. The key is deleted from memory either at the end of OIM session or after 30 minutes of inactivity.

After a subscriber's identity is vetted and his/her request for a certificate is granted, the subscriber starts a session with the OIM server. During the session, the OIM server generates the certificate signing request and sends it to the CA. As soon as the request is signed, the OIM server creates a PKCS12 object that includes the certificate and the private key and makes this available for the subscriber's download. After the subscriber downloads the PKCS12 file, the session ends. Usually, a session is completed in a few minutes. The user's private key is never sent to the CA and only kept on OIM server for a maximum of 30 minutes.

6.1.2 Private key delivery to subscriber

After a subscriber's identity is vetted and his/her request for a certificate is granted, the subscriber starts a session with the OIM server. The subscriber is authenticated by his/her password chosen in the enrollment phase. During the session, the OIM server generates and sends a certificate signing request to the CA. As soon as the request is signed, the OIM server creates a PKCS12 object that includes the certificate and the private key and makes this available for the subscriber's download. The subscriber downloads the PKCS12 file on his/her local disk and this concludes the session. The session between the subscriber and the server is protected by the TLS protocol and the OIM server at all times has a valid service certificate.

For the command line tools that are used for certificate request and renewal, the key pair is generated by the subscriber and never leaves the local disk.

6.1.3 Public key delivery to certificate issuer

In the case where the subscriber generates the public key to be certified, the subscriber delivers his or her public key, in a certificate request signed by the corresponding private key, to the CA, in a TLS encrypted session.

6.1.4 CA public key delivery to relying parties

The root CA certificate is provided to the International Grid Trust Federation (IGTF) for inclusion in the IGTF Trust Anchor Distribution. It is also published in the CA repository (Section 2.2).

6.1.5 Key sizes

CA and end entity keys will use a 2048 bit RSA modulus.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

Certificate extensions, including key usage flags, are specified in Section 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The CA stores private keys in cryptographic hardware security modules certified at FIPS 140-2 level 3 and operated in FIPS 140 level 3 mode.

6.2.2 Private key (n out of m) multi-person control

The CA private key is not under n out of m multi-person control.

6.2.3 Private key escrow

The CA private key is not escrowed.

6.2.4 Private key backup

The CA private key is stored in multiple cryptographic hardware security modules for redundancy.

The CA private key is backed up in encrypted form on offline media stored in a locked cabinet in the University of Illinois office of a CA operator. The pass phrase of the encrypted private key is stored in a sealed envelope stored in a

separate locked cabinet in the University of Illinois office of a separate CA operator.

6.2.5 Private key archival

The CA private key is not archived.

6.2.6 Private key transfer into or from a cryptographic module

CA operators transfer encrypted CA private keys from offline media into the cryptographic hardware security modules at the time of key pair generation (Section 6.1.1) or in the case that a new cryptographic hardware security module is added to the CA system. Private keys are never transferred from a cryptographic module.

6.2.7 Private key storage on cryptographic module

The CA stores private keys on cryptographic modules in non-exportable form.

6.2.8 Method of activating private key

The CA system activates private keys in the cryptographic modules automatically on power on. Keys are activated for an indefinite period.

6.2.9 Method of deactivating private key

CA operators can deactivate the private key by powering off the cryptographic module or using the operator interface to mark the key inactive.

6.2.10 Method of destroying private key

CA operators can destroy the private key in the cryptographic module by reinitializing the device (i.e., restoring it to factory default settings).

6.2.11 Cryptographic Module Rating

The cryptographic hardware security modules meet FIPS 140-2 level 3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All issued certificates (which contain public keys) are archived for at least three years.

6.3.2 Certificate operational periods and key pair usage periods

End entity certificates have a maximum lifetime of 13 months.

CA certificates have a maximum lifetime of 20 years.

6.4 Activation data

6.4.1 Activation data generation and installation

CA operators use cryptographic module software and procedures to generate and install activation data on CA servers that allows the CA servers to submit certificate requests to the cryptographic modules for signing.

6.4.2 Activation data protection

Cryptographic module activation data resides on the local CA server file system, protected by operating system permissions.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The CA system consists of front-end web application servers, back-end CA signing servers, and cryptographic hardware security modules. The front-end web application servers accept HTTP (port 80) and HTTPS (port 443) connections from the Internet, serving CRLs over HTTP and certificate requests over HTTPS. The front-end web application servers connect to the back-end CA signing servers via private links. The back-end CA signing servers process approved signing requests and log all certificate issuances. The back-end CA signing servers connect to cryptographic hardware security modules via TLS, authenticated using the activation data described in Section 6.4. The CA systems are located on a highly protected/monitored network and are actively monitored for intrusions. The backend CA signing servers and cryptographic hardware security modules only run the necessary CA software for proper functioning. The frontend web application server only provides the OIM server.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

All CA systems employ operating system firewalls allowing inbound connections only for required CA services. CA systems are connected to highly protected networks, which are actively monitored for intrusions.

6.8 Time-stamping

CA servers maintain accurate system clocks via trusted NTP servers.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

End entity certificates comply with RFC 5280 and GFD.125.

7.1.1 Version number(s)

The X.509 certificate version number is 2 indicating a Version 3 certificate.

7.1.2 Certificate extensions

The self-signed CA certificate contains the following extensions:
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier
X509v3 Authority Key Identifier
X509v3 Subject Alternative Name:
email:ca@cilogon.org

End entity personal certificates contain the following extensions:
X509v3 Basic Constraints: critical

CA:FALSE
X509v3 Key Usage: critical
Digital Signature, Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.34998.1.6.2
Policy: 1.2.840.113612.5.2.2.1
X509v3 CRL Distribution Points:
URI:http://crl.cilogon.org/cilogon-osg.crl
X509v3 Subject Alternative Name:
email:username@example.org

End Entity Host/Service certificates contain the following extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage: critical
Digital Signature, Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server, TLS Web Client Authentication
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.34998.1.6.2
Policy: 1.2.840.113612.5.2.2.1
X509v3 CRL Distribution Points:
URI:http://crl.cilogon.org/cilogon-osg.crl
X509v3 Subject Alternative Name:
DNS:test.example.edu, email:test@example.edu

7.1.3 Algorithm object identifiers

Hash Functions: sha256 2.16.840.1.101.3.4.2.1
RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
Signature Algorithms: sha256WithRSAEncryption 1.2.840.113549.1.1.11

7.1.4 Name forms

See Section 3.1.1.

7.1.5 Name constraints

All end entity subject distinguished names have the following prefix: /DC=org/DC=opensciencegrid

7.1.6 Certificate policy object identifier

End entity certificates contain the following policy OIDs:

1.3.6.1.4.1.34998.1.6.2	CILogon OSG CA CP/CPS (this document)
1.2.840.113612.5.2.2.1	Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure

7.1.7 Usage of Policy Constraints extension

Not used.

7.1.8 Policy qualifiers syntax and semantics

Not used.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

CRLs comply with RFC 5280.

7.2.1 Version number(s)

The CRL version number is 1 indicating a Version 2 CRL.

7.2.2 CRL and CRL entry extensions

CRLs contain the following extension: X509v3 CRL Number

7.3 OCSP profile

The CA does not support OCSP.

7.3.1 Version number(s)

Not applicable.

7.3.2 OCSP extensions

Not applicable.

8. COMPLIANCE AUDIT AND OTHER

ASSESSMENTS

8.1 Frequency or circumstances of assessment

The CA performs internal operational audits at least once per year to verify compliance with the rules and procedures specified in this document.

A list of CA operators is maintained and verified at least once per year.

The CA performs audits over a random set of RA Agents annually.

The CA consents to external audits and makes logs available for viewing by external auditors.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

CA audit results are made available to the TAGPMA upon request.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The CA does not charge certificate issuance or renewal fees.

9.1.2 Certificate access fees

The CA does not charge certificate access fees.

9.1.3 Revocation or status information access fees

The CA does not charge revocation or status information access fees.

9.1.4 Fees for other services

The CA does not charge fees for other services.

9.1.5 Refund policy

The CA does not give refunds.

9.2 Financial responsibility

The CA accepts no financial responsibility.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

Information and data maintained in electronic media on University of Illinois computer systems are protected by the same laws and policies, and are subject to the same limitations, as information and communications in other media. Before storing or sending confidential or personal information,

subscribers should understand that most materials on University systems are, by definition, public records. As such, they are subject to laws and policies that may compel the University to disclose them. The privacy of materials kept in electronic data storage and electronic mail is neither a right nor is it guaranteed.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

The contents of certificates and CRLs are not deemed private.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This policy is in effect during the validity period of certificates issued under it.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

The procedure for amending this document is as follows:

- Increment the document version number and date in title page and Section 1.2.
- Increment the Policy OID version number in title page, Section 1.2, Section 2.2, Section 7.1.2, and Section 7.1.6.
- Make changes to the document text.
- Document changes in the revision history in Section 1.2.
- Publish the updated document at OSG Certificate Service.
- Publish a PDF highlighting changes from the last version at OSG Certificate Service.
- Announce the policy changes to tagpma-general@tagpma.org.
- Allow a two week comment period. Incorporate comments and update the document as necessary.
- Update the CA configuration to include the new Policy OID in issued certificates.

9.12.2 Notification mechanism and period

Any modifications to this policy must be published/announced at least two weeks prior to their taking effect.

9.12.3 Circumstances under which OID must be changed

The version number in the Certificate Policy OID must be incremented upon any significant change in policy.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.