CILogon OpenID Certification Authority Certificate Policy and Certification Practice Statement (CP/CPS)

December 3, 2014

Version 4
1.3.6.1.4.1.34998.1.3.4

http://ca.cilogon.org/policy/openid

Contents

1. INTRODUCTION

1.1 Overview

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

The CA issues end entity certificates to users of the US National Science Foundation cyberinfrastructure. Identification and authentication of certificate applicants is performed by OpenID.

Subscribers obtain a certificate from the CA according to the following process. First, the subscriber authenticates (via a web browser) to his or her OpenID provider, which issues a signed OpenID authentication assertion to the CA web service (via a web browser redirect). Then, the CA web service validates the authentication assertion, and if valid, assigns an X.500 distinguished name to the subscriber based on the Identifier and user profile data provided by the OpenID provider. Finally, the CA issues a signed X.509 certificate containing the subject distinguished name to the subscriber.

1.2 Document name and identification

Name: CILogon OpenID Certification Authority Certificate Policy and Practice Statement
Version: 4
Date: December 3, 2014
ASN.1 object identifier: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1) CILogon Project (34998) Certificate Policies (1) CILogon OpenID CA (3) Version (4)

Revision history:

1. Jun 2 2010: Initial version.
2. Feb 3 2011: Allow subscriber private keys to be generated by the CA and delivered securely to subscribers (Section 4.1.2). Update CA certificate locations (Section 2.2) and CRL locations (Section 4.10 and 7.1.2). Document additional personnel controls in Section 5.3. Add SHA-2 OIDs in Section 7.1.3.
3. Mar 31 2011: Update subject name template to include OpenID provider name, subscriber name, and UID, similar to CILogon Basic/Silver CAs, rather than constructing the certificate subject just with the OpenID Identifier (Section 3.1.1).
4. Feb 4 2014: Increase CRL validity period from two weeks to 30 days (Section 2.3). Added ORNL site information (Section 5.1).

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 OpenID.

1.3.3 Subscribers

The subscribers of the CA are the users of the US National Science Foundation cyberinfrastructure.

1.3.4 Relying parties

The relying parties of the CA are the US National Science Foundation cyberinfrastructure providers 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 US National Science Foundation cyberinfrastructure.

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 CILogon Policy Management Authority (pma@cilogon.org).

1.5.2 Contact person

Jim Basney
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
1205 West Clark Street
Urbana, Illinois 61801 USA
jbasney@cilogon.org
Voice: +1 217-244-1954
Fax: +1 217-244-1987

For inquiries and fault reporting, contact ca@cilogon.org.

1.5.3 Person determining CPS suitability for the policy

This combined CP/CPS is administered by the CILogon Policy Management Authority (pma@cilogon.org), which determines its suitability.

1.5.4 CPS approval procedures

The CILogon Policy Management Authority approves CP/CPS changes by consensus of its members.

1.6 Definitions and acronyms

No stipulation.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The CA publishes information regarding its practices, certificates, contact information, etc., at http://ca.cilogon.org/.

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:

http://ca.cilogon.org/	web page of the CA for general information
http://ca.cilogon.org/cilogon-openid-policy.pdf	the current version of this policy
https://cilogon.org/cilogon-openid.pem	self-signed PEM-formatted CA certificate
https://cilogon.org/cilogon-openid.crt	self-signed DER-formatted CA certificate
http://crl.cilogon.org/cilogon-openid.r0	PEM-formatted CRL
http://crl.cilogon.org/cilogon-openid.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 (ca@cilogon.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.

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.

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 OpenID CA 1

The CA updates the issuer CN in case of key changeover (Section 5.6), so that each "CILogon OpenID 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 all certificates is:

/DC=org/DC=cilogon/C=US/O=*OpenIDProvider*/CN=*EndEntityName UID*

In the above template:

- *OpenIDProvider* is an identifier for the OpenID Provider ("Google", "Yahoo", "Verisign", etc.).
- *EndEntityName* is a presentation of the subject's name provided by the OpenID Provider in OpenID namePerson, fullname, or similar attributes.
- *UID* is a unique numeric identifier for the subscriber, assigned by the CA, to ensure uniqueness of subject names (see Section 3.1.5).

For example:

/DC=org/DC=cilogon/C=US/O=Google/CN=Jim Basney A437

The subject alternative name (subjectAltName) extension contains an Internet mail address of type rfc822Name (for example: jbasney@cilogon.org) from the OpenID email attribute.

3.1.2 Need for names to be meaningful

The commonName (CN) component contains the subscriber's name, as provided by the OpenID provider. The subject alternative name contains the subscriber's contact email address as provided by the OpenID provider.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity is determined by the subscriber and his or her OpenID provider.

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.

3.1.5 Uniqueness of names

Subjects are uniquely identified by their OpenID Identifier, which determines the unique numeric identifier (UID) that the CA assigns to each subscriber and includes in the certificate subject.

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. This requirement does not apply in the case the CA generates a keypair on the subscriber's behalf.

3.2.2 Authentication of organization identity

The CA does not authenticate organization identity.

3.2.3 Authentication of individual identity

The subscriber's chosen OpenID Provider is responsible for authenticating the subscriber's individual identity (i.e., the OpenID Identifier).

The CA makes no claim regarding the strength of this authentication.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

The CA performs no validation of authority.

3.2.6 Criteria for interoperation

The CA interoperates 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

Certificate re-key is not supported. Instead, subscribers should submit a new certificate application, which will be authenticated according to Section 3.2.

3.3.2 Identification and authentication for re-key after revocation

Certificate re-key is not supported. Instead, subscribers should submit a new certificate application, which will be authenticated according to Section 3.2.

3.4 Identification and authentication for revocation request

Revocation requests from subscribers must be authenticated by one of the following methods:

- The digital signature on the request matches the certificate to be revoked.
- The subscriber submitted the revocation request in a TLS or OpenID authenticated web session, and the authenticated TLS/OpenID identity matches the certificate to be revoked.

In any case, proof of compromise or exposure of a private key is sufficient justification for CA operators to revoke the corresponding certificate.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any person may submit a certificate application. Certificate applications must be submitted by the certificate subject (i.e., the person identified in the certificate) or a software process acting on the subject's behalf (i.e., initiated by the subject), and may not be submitted by a registration authority or other third party on the subject's behalf.

4.1.2 Enrollment process and responsibilities

Subscribers obtain a certificate from the CA according to either of the following two enrollment process options, which differ with respect to keypair generation. All network communication occurs over encrypted HTTPS connections, with server identity verification, according to to RFC 2818.

In the first option, the subscriber generates the key pair. First, the subscriber authenticates (via a web browser) to his or her OpenID provider, which issues a signed OpenID authentication assertion to the CA web service (via a web browser redirect). Next, the subscriber (i.e., software running on the subscriber's behalf) generates a 2048 bit RSA key pair and submits a certificate request containing the 2048 bit RSA public key to the CA web service. Finally, if the CA approves the request (according to Section 4.2.2), the CA web

service returns a signed X.509 certificate containing the public key and subject distinguished name to the subscriber. Otherwise, if the CA rejects the request (i.e., any of the conditions in Section 4.2.2 are unmet), the CA web service will not return a signed certificate but will instead return an error message to the subscriber.

In the second option, the CA generates the key pair and delivers it securely to the subscriber. First, the subscriber authenticates (via a web browser) to his or her OpenID provider, which issues a signed OpenID authentication assertion to the CA web service (via a web browser redirect). Next, the CA web service prompts the subscriber to enter a private key pass phrase of at least 12 characters in length. Then, if the CA approves the request (according to Section 4.2.2), the CA web service generates a 2048 bit RSA key pair and a signed X.509 certificate containing the public key and subject distinguished name for the subscriber, bundles them in a PKCS12 object that is encrypted with the subscriber-chosen pass phrase, and delivers the PKCS12 object to the subscriber. The CA web service securely destroys all its copies of PKCS12 objects within 15 minutes of their creation. If instead the CA rejects the request (i.e., any of the conditions in Section 4.2.2 are unmet), the CA web service will not generate a key pair or certificate but will instead return an error message to the subscriber.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The CA web service validates the signed OpenID authentication assertion.

4.2.2 Approval or rejection of certificate applications

The CA approves certificate applications if all of the following criteria are met:

- The subscriber submits the certificate application in an OpenID authenticated and TLS secured web session.
- The digital signature on the OpenID assertion is valid.
- The OpenID assertion contains an Identifier (see Section 3.1.1).
- In case the subscriber provides a certificate request, it must be digitally signed by the private key associated with the 2048 bit RSA public key in the request (see Section 3.2.1).

Otherwise, the certificate application will be rejected.

4.2.3 Time to process certificate applications

Certificate applications are processed automatically. Approved applications result in automatic (i.e., immediate) certificate issuance. Non-approved applications are automatically rejected. All certificate applications (approved and non-approved) are logged.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon approval of a certificate application, the CA assigns an X.500 distinguished name to the subscriber based on the identifying information in the authentication assertion (see Section 3.1) and issues a signed X.509 certificate containing the subscriber's public key and subject

distinguished name.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA delivers the issued certificate to the subscriber through the software process the subscriber used to apply for the certificate.

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

4.7.1 Circumstance for certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

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 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.

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 ca@cilogon.org.

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 must process 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-basic.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 on the CA web site (http://ca.cilogon.org/).

The DOEGrids CA graciously hosts a backup CRL distribution point at http://crl.doegrids.org/cilogon-basic.crl that provides continuity of service in case of cilogon.org outages.

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 CITES storage facility in Rantoul, Illinois.

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 of Illinois 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 at http://docs.cilogon.org.

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

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 (CITES and NCSA)
- National Science Foundation program officers
- National Science Foundation cyberinfrastructure project incident response teams

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 University of Illinois 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

Business continuity plans and capabilities are under development.

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).

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

End entity private keys may be generated by subscribers or by the CA, according to Section 4.1.2. In either case, private keys must be generated and protected according to the IGTF Guidelines on Private Key Protection.

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). A member of the CILogon PMA supervises the CA private key generation process and records 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.

6.1.2 Private key delivery to subscriber

In the case when the CA, rather than the subscriber, generates the private key, according to Section 4.1.2, the CA delivers the private key to the subscriber in a PKCS12 object that is encrypted with a subscriber-chosen pass phrase and sent to the subscriber over an encrypted HTTPS session.

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 SAML authenticated TLS encrypted session according to the certificate application process (Section 4.1).

6.1.4 CA public key delivery to relying parties

The root CA certificate is 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 safe in the University of Illinois office of the CILogon PMA chair. 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 CILogon PMA member.

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 filesystem, 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 (with OpenID authentication). 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. All CA systems are dedicated machines, running no other services than those needed for CA operations. The CA systems are located on a highly protected/monitored network and are actively monitored for intrusions.

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 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
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.34998.1.3.4
X509v3 CRL Distribution Points:
URI:http://crl.cilogon.org/cilogon-openid.crl
URI:http://crl.doegrids.org/cilogon-openid.crl
X509v3 Subject Alternative Name:
email:username@example.org

7.1.3 Algorithm object identifiers

Hash Functions: sha1 1.3.14.3.2.26, sha256 2.16.840.1.101.3.4.2.1, sha384 2.16.840.1.101.3.4.2.2, sha512 2.16.840.1.101.3.4.2.3
RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
Signature Algorithms: sha1WithRSAEncryption 1.2.840.113549.1.1.5, sha256WithRSAEncryption 1.2.840.113549.1.1.11, sha384WithRSAEncryption 1.2.840.113549.1.1.12, sha512WithRSAEncryption 1.2.840.113549.1.1.13

7.1.4 Name forms

See Section 3.1.1.

7.1.5 Name constraints

All distinguished names have the following prefix:
/DC=org/DC=cilogon/C=US

7.1.6 Certificate policy object identifier

End entity certificates contain the following policy OID:

1.3.6.1.4.1.34998.1.3.4	CILogon OpenID CA CP/CPS (this document)

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)

No stipulation

7.3.2 OCSP extensions

No stipulation.

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.

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 CILogon PMA.

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 7.1.2, and Section 7.1.6.

- Make changes to the document text.
- Document changes in the revision history in Section 1.2.
- Announce the policy changes to pma@cilogon.org.
- Publish the updated document at http://ca.cilogon.org/cilogon-openid-policy.pdf and http://ca.cilogon.org/policy.
- Publish a PDF highlighting changes from the last version at http://ca.cilogon.org/policy.
- Announce the policy changes at http://ca.cilogon.org/news.
- 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

The laws of the United States of American and the State of Illinois, where this CA is established, govern the interpretation of this policy.

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

This material is based upon work supported by the National Science Foundation under grant number 0943633. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.