# DOE Grids CA
# Certificate Policy
# and
# Certification Practice Statement
# Version 2.10

Editor: Michael Helm

Michael Helm 12345

Digitally signed by Michael Helm 12345
DN: dc=org, dc=doegrids, ou=People, cn=Michael Helm 12345
Date: 2008.09.03 12:38:48 -07'00'

March 28, 2008

# Table of Contents

# 1 Introduction

## *1.1 Overview*

This document is structured according to RFC 2527 [RFC2527]. Not all sections of RFC 2527 are used. Sections that are not included have a default value of "No stipulation".

This document describes the set of rules and procedures established by the DOE Grids Policy management Authority for the operations of the DOE Grids PKI service. ESnet operates the DOE Grids Public Key infrastructure under the authority of the DOE Grids PMA. ESnet and the data center housing the PKI servers are located at Lawrence Berkeley National Laboratory, Berkeley, California.

This document will include both the Certificate Policy and the Certification Practice Statement for the DOE Grids PKI. The general architecture is a certificate authority with multiple Registration Authorities. The certificate authority is a subordinate of the ESnet root CA. There is a Registration Authority for each DOE GRIDS site or Virtual Organization. Each Registration Authority is responsible for the vetting of user identities of their community. Special guidelines for the individual RAs of the DOE GRIDS PKI are covered in the specific VO or Site Appendixes in this document.

DOEGrids PKI is a Traditional X.509 Public Key Certification Authority that complies with the IGTF Profile for a traditional X.509 Public Key Certification Authorities with secure infrastructure, version 4.0. It is the intent of the DOE Grids PKI to issue Identity and service certificates for use in Grids. These certificates are for DOE researchers and their colleagues. These certificates will be compatible with the Globus middleware that is used on these Grids.

The DOEGrids personal certificates by themselves are not to be used for determining Authorization. The DOEGrids personal certificate can be used only to assert the identity of the individual it was assigned to. Authorization decisions must be based on other criteria then the DOEGrids personal certificate.

### 1.1.1 General Definitions

**Activation Data**

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

**Certification Authority (CA)**

The entity / system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA

**Certificate Policy (CP)**

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

**Certification Practice Statement (CPS)**

A statement of the practices, which a certification authority employs in issuing certificates.

**Community RM**
One or more RMs that serve multiple, low request rate, sites / Virtual Organizations.

**DOE Grids PKI**
Refers to the whole of the PKI including the electronic services, the CA managers, RA's, RAg's.

**DOE Grids PKI members**
Refers to the CA managers and the RA Points of Contact, who comprise a large subset of the PMA.

**DOE Grids PKI service**
Refers to the electronic services of the PKI, computers, web interfaces, email, etc.

**End Entity**
A system entity or person that is the subject of a public-key certificate and that is permitted and able to use, the matching private key only for a purpose or purposes other than signing an X.509 public key certificate; i.e., an entity that is not a CA.

**Host Certificate**
A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites/VOs

**Owner**
The human individual or organizational group that has valid rights to exclusive use of a subject name in a certificate. The process of registering the end entity of a certificate request is what maintains the binding between an owner and the subject name (DN).

**Person Certificate**
A certificate associated with a unique human being.

**Policy Management Authority (PMA)**
For the DOEGrids PKI this is a committee composed of the CA managers and representatives from the site/VO Registration Authorities. The PMA has direct responsibility for the CP/CPS and oversight of ESnet operations of the PKI.

**Policy Qualifier**
The policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

**Point of Contact**
The member of a site/VO RA that has been chosen to handle all communications about policy matters with the DOE GRIDS PMA.

**Private RM**
RMs that serve high certificate request rate sites / Virtual Organizations, and that are operated by the site/VO.

**Registration Authority (RA)**
An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

**Registration Agent (RAg) or "Agent"**
RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.

**Registration Manager (RM)**
The RM is a front-end Web server for the CA that provides a Web user interface for CA subscribers and agents. The RM forwards certificate-signing requests to the actual CA (DOE GRIDS) to issue X.509 certificates.

**Registered Owner**
Once a certificate request has been verified, the ownership of the DN validated, and a certificate issued, the owner is considered to be the "registered owner" of the DN. See above for definition of "Owner".

**Relying Party**
A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

**Security Incident**
An incident that has the potential of private key loss or compromise, regardless of if the compromise or loss was successful. Such incidents include but are not limited to user credential compromise, privilege escalation on systems known to contain private keys, accidental exposure of private keys to unauthorized third parties or loss of a private key.

**Service Certificate**
A certificate for a particular service running on a host. It will represent a single service on a single host.

**Set of provisions**
A collection of practice and/or policy statements, spanning a range of standard topics, for use in +expressing a certificate policy definition or CPS and employing the approach described in this framework.

**Subscriber**
The person that applied for and was issued a certificate.

**Virtual Organization (VO)**
An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at. (i.e. PPDG, FNC, EDG, etc).

## *1.2 Identification*

Document title: DOE Grids CA Certificate Policy and Certification Practice Statement

Document version: 2.10

Document date: March 28, 2008

OID: [ESnet].ERmember.DOEGrids.CP-CPS.CPVersionNumber.CPReleaseNumber

1.2.840.113612.3.7.1.2.10

## *1.3 Community and Applicability*

### 1.3.1 Certification Authorities

ESnet will manage and operate the DOEGrids PKI. The DOEGrids CA is operated as a subordinate CA of the ESnet Root CA. Access to the DOEGrids CA Certificate Management Service is by a web browser. Web browsers or other client software is the responsibility of the client, not ESnet. Check the FAQ on the www.DOEGrids.org site for the list of supported browsers. The following is a list of the PKI components:

| Component | Location | Function |
|---|---|---|
| ESnet Root CA | ESnet Data Center | Signs subordinate CAs |
| DOE Grids CA | ESnet Data Center | Signs Subscriber, host and Service Certificates |
| DOE Grids Community RM | ESnet Data Center | Creates Certificate Signed Requests, Agents use to approve certificate requests |
| DOE Grids LDAP directory | ESnet Data Center | The DOE Grids CA publishes certificates and other information to the directory. The directory is public and read only. |
| Subscriber Web browsers | Subscriber Desk tops | This is the standard Subscriber interface to the RM. It is also used by Agents for reviewing Certificate requests. The LDAP Directory also provides a web interface. |

### 1.3.2 Registration Authorities

The DOE Grids PKI consists of a number of individual RAs representing a DOE site or Virtual organization (VO). ESnet maintains a browser accessible shared community Registration Manager for use by the DOE Grids RAs. This interface can be used to:

- Approve or Reject the certificate request
- Initiate certificate revocations
- Search for certificates

See the RA appendices for more detailed definition of the community and practices of each RA.

### 1.3.3 End Entities

DOE GRIDS PKI issues Person, Host and Service certificates to scientists, engineers, graduate students, and others working on Department of Energy Scientific Research programs as allowed in the ESnet AUP (http://es.net/hypertext/esnet-aup.html), or as allowed by the DOE Office of Science in support of DOE collaborations with other agencies and institutions. The person requesting and responsible for a certificate's private key is the *subscriber*. The term *end entity* is used to refer to the holder of the private key. For a person certificate it will be the subscriber, but for a host or service certificate the end entity may be some process running on a machine.

### 1.3.4 Applicability

See section 1.1.1 for definition of certificate types.

***Person certificates*** can be used to authenticate a person to relying sites that have agreed to accept certificates from the DOE Grids CA. This authentication may require the signing of Globus proxy certificates. It is expected that these sites will be supported by DOE funding or will be collaborating with such sites. While Person certificates may be used for other activities such as e-mail signing and encryption, these are not supported

activities. These certificates are not suitable for legally binding digital signatures on documents.

***Service certificates*** can be used to identify a named service on a specific host and for encryption of communication (TLS/SSL).These certificates may be used to authenticate the service to another Grid entity, possibly by signing Globus proxy certificates.

## *1.4 Contact Details*

DOE GRIDS PKI is operated by **ESnet** and managed by a Policy Management Authority. The members of the PMA can be found on the project web site (http://www.doegrids.org/pages/doegridspma.html)

Contact person for questions related to this document is the chairman of the PMA. The PMA chairman (acting) and his/her contact information:

Robert Cowles

Stanford Linear Accelerator Center

Email: rdc@slac.stanford.edu

The acting custodian of this document is:

Michael Helm
ESnet/LBNL
One Cyclotron Road, B50A 3131
Berkeley, CA 94706
phone: +1 510 486 7248
E-mail: helm@es.net

Contact information regarding other communications with the DOEGrids PKI, including security incidents, is maintained at http://www.doegrids.org/
The following email addresses and phone numbers can be used to request information or report problem (Security, access or service failures) Security incidents, access problems or other service failures should be reported to ESnet's trouble reporting service:

ESnet Trouble email: trouble@es.net

ESnet Trouble Numbers:

1 800 33-ESnet
1 800 333-7638
(toll free within the United States)

+1 510 486-7600
(outside the United States)

# 2 General Provisions

## *2.1 Obligations*

All RA, agents, subscribers are all obliged to notify the CA and their RA when their status changes. Status changes that affect certification include among other things change of:

1. Contact email address
2. Name
3. No longer covered by ESnet AUP or interoperability agreement.

DOEGrids PMA has defined a number of roles that together provide the service to the community. The following roles have been defined:

- Certificate Authority Operations
  - Responsible for the day to day operations of the CA
  - It has the authority to issue and revoke certificates as needed to run the service.
- Registration Authority
  - Responsible for the vetting of EE identities for certificates
- RA Agent
  - Acts on behalf of the Registration Authority and is responsible to the RA.
- Grid Admin
  - Acts on behalf of the Registration Authority, but is limited to a defined domain of hosts.

This section describes the top level obligations for the CA Operator and RA. Appendix A has additional details for RAs, Agents and Grid Admins. Appendix M has details for CA operations.

### 2.1.1 CA and RA Obligations

**DOE GRIDS CA** will:

1. Accept certification requests from entitled entities;
2. Notify the RA of certification request and accept authentication results from the RA.
3. Issue certificates based on the requests from authenticated entities;
4. Maintain the binding between DN and registered owner of the DN. One attribute of this binding is the email address included in the certificate.
5. Notify the subscriber of the issuing of the certificate;
6. Publish the issued certificates;
7. Accept revocation requests according to the procedures outlined in this document, and notify the RA that issued the certificate;
8. Authenticate entities requesting the revocation of a certificate, possibly by delegating this task to a DOE GRIDS RA;
9. Issue a Certificate Revocation List (CRL);
10. Publish the CRL issued.
11. Keep audit logs of the certificate issuance process
12. Notify the RA of security incidents that have been reported and coordinate incident response between it and the RA.
13. Publish contact information for the CA.
14. Notify RA Points of Contact whenever contact information for the CA changes.

**A DOE GRIDS RA** will:

1. Accept authentication requests from the DOE GRIDS CA;
2. Authenticate entity making the certification request according to procedures outlined in this document;
3. Verify that the person making the request is permitted by the community guidelines and ESnet AUP.
4. Verify that entity making request is the registered owner if the DN exists previous to this request and resolve conflicts or manage transfer of DN ownership.
5. Notify the DOE GRIDS CA when authentication is completed for a certification or revocation request;
6. Accept revocation requests according to the procedures outlined in this document;
7. Notify the DOE GRIDS CA of all revocation requests;
8. Authenticate entity making revocation request according to procedures outlined in this document or the specific Appendix in this document that represents the Virtual Organization or DOE Site.
9. Maintain a record of authentication of entities for certification and revocation requests, for a minimum of three years.
10. Will not approve a certificate with a life time greater then 12 months. Each VO/Site will specify the life time of their certificates in their specific appendix.
11. Additional guidelines are described in Appendix A and the individual VO Appendix included in this document.
12. Notify CA of security incidents. Notification should be made as soon as possible, ideally within 12 hours of initial knowledge of incident.
13. Publish contact information for the RA
14. Notify the CA whenever the contact information for the RA changes.

### 2.1.2 Subscriber Obligations

Subscribers must:

1. Read and adhere to the procedures published in this document;
2. Read and adhere to the ESnet Acceptable Use Policy (http://es.net/hypertext/esnet-aup.html)
3. Generate a key pair using a trustworthy method;
4. Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:

For Person Certificates

Selecting a pass phrase of at minimum 8 characters

Protecting the pass phrase from others

Always using the pass phrase to encrypt the stored private key.

Never sharing the private key with other users.

For Service Certificates

1. Storing them encrypted whenever possible.
2. They may be kept unencrypted on the host that they represent.
3. Assert that they are authorized to run install the specified service on the specified host.

4. Provide correct personal information and authorize the publication of the certificate
5. Verify that the DN being requested does not yet exist, or assert that they are the registered owner of the DN.
6. Notify DOE GRIDS PKI immediately of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of incident.
7. Use the certificates for the permitted uses only.

### 2.1.3 Relying Party Obligations

Relying parties must:

- Read the procedures published in this document;
- Use the certificates for the permitted uses only.
- Do not assume any authorization attributes based solely on an entity's possession of a DOE GRIDS certificate.
- Notify DOE Grids PKI of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of incident.

Relying parties may:

Verify that the certificate is not on the DOEGrids CRL before validating a certificate;

### 2.1.4 Repository Obligations

DOE GRIDS PKI will provide access to DOE GRIDS CA information, as outlined in section 2.6.1, on its web site. The following pages deal with individual items from 2.6.1:

CA information: http://www.doegrids.org/pages/Fingerprints.htm

Certificates: LDAP access: ldap://ldap.doegrids.org

CRL information: http://pki1.doegrids.org/CRL/1c3f2ca8.r0

CP/CPS: http://www.doegrids.org/Docs/CP-CPS.pdf

## *2.2 Liability*

DOE GRIDS PKI and its agents issue person certificates according to the practices described in this document to validate identity. No liability, implicit or explicit, is accepted.

DOE GRIDS PKI and its agents make no guarantee about the security or suitability of a service that is identified by a DOE GRIDS certificate. The certification service is run with a reasonable level of security, but it is provided on a *best effort only* basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

DOE GRIDS PKI denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

## *2.3 Financial Responsibility*

No Financial responsibility is accepted.

## *2.4 Interpretation and Enforcement*

### 2.4.1 Governing Law

This policy is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders and Lawrence Berkeley National Laboratory management directives.

## *2.5 Fees*

No fees are charged for DOE GRIDS Certificates. All costs for operation are covered directly or indirectly by DOE.

## *2.6 Publication and Repositories*

### 2.6.1 Publication of CA information

DOE GRIDS PKI will operate a secure online repository that contains:

- DOE GRIDS CA's certificate;
- Certificates issued by the PKI;
- A Certificate Revocation List;
- A copy of this policy
- Other information deemed relevant to the DOE GRIDS PKI.

### 2.6.2 Frequency of Publication

- Certificates will be published to the DOE GRIDS PKI repository as soon as issued.
- CRLs will be published as soon as issued or refreshed once every month if there are no changes.
- All DOE GRIDS PKI documents will be published to the project website as they are updated.

### 2.6.3 Access Controls

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.

DOE GRIDS PKI does not impose any access control on its Policy, its signing Certificate and issued certificates, and its CRLs. In the future, DOE GRIDS PKI may impose access controls on issued certificates, their status information and CRLs at its discretion, subject to agreement between the CA, relying parties and subscribers.

### 2.6.4 Repositories

Repository of certificates and CRLs can be found in the service's LDAP directory: LDAP.doegrids.org or on its website www.doegrids.org:

CA certificate:

ldap://ldap.doegrids.org/ CN=DOEGrids CA 1, OU=Certificate Authorities, DC=DOEGrids, DC=org : cacertificate: <attribute value>

http://www.doegrids.org/CA/DOEGrids%20CA%201

CRLs:

ldap://ldap.doegrids.org/ CN=DOEGrids CA 1, OU=Certificate Authorities, DC=DOEGrids, DC=org: certificaterevocationlist: <attribute value>

http://{www.}doegrids.org/CA/DOEGrids CA 1

CP/CPS:

http://www.doegrids.org/CA/DOEGrids%20CA%201/Certificate%20Policy.pdf

Third party repositories are maintained by the EUGridPMA (www.EUGridPMA.org) and TERENA Academic CA Repository (https://www.tacar.org/). These repositories maintain trusted copies of the following information:

- ESnet Root CA certificate
- DOEGrids CA certificate
- Links to the CRLs for each CA

Links to our CP/CPS

## 2.7 Compliance audit

The DOE GRIDS PKI is not audited by an outside party. The CA operation may be reviewed by any cross certifying organization or potential relying organization if approved by the PMA.

## 2.8 Confidentiality

DOE GRIDS PKI collects subscribers' full names and e-mail addresses. Some of this information is used to construct unique, meaningful subject names in the issued certificates.

Information included in issued certificates and CRLs is **not** considered confidential.

DOE GRIDS PKI does not collect any kind of confidential information.

DOE GRIDS PKI does not have access to or generate the private keys of a digital signature key pair, such as those used in DOE GRIDS identity certificates. These key pairs are generated and managed by the client and are the sole responsibility of the subscriber.

## 2.9 Intellectual Property Rights

Parts of this document are inspired by [INFN CP], [GridCP], [EuroPKI], [TrustID] , [NCSA] , [PAG] and [FBCA].

# 3 Identification and Authentication

## *3.1 Initial Registration*

### 3.1.1 Types of names

Name components vary depending on the type of certificate. Names will be consistent with the name requirements specified in RFC2459. See section 7.1.4 for more details.

### 3.1.2 Name Meanings

For individuals, the value of the CN component of the DN has no semantic significance. It should have a reasonable association with the authenticated name of the subscriber. For Hosts or Services, the CN component has a structure that is defined to support SSL/TLS and the Globus software. It should include the Fully Qualified Domain Name (FQDN) of the host.

### 3.1.3 Uniqueness of names

The Distinguished Name must be unique for each subject name certified by the DOE GRIDS PKI.

For person certificates each CN component will include the Full name of the subscriber as determined by the Virtual Organization/Site's RA. The registration interface appends 5 or 6 random alphanumeric characters (i.e. "John K. Doe 1W2D3") when constructing the Common Name to assist in establishing uniqueness. Certificates must apply to unique individuals or resources. Private keys associated with Person certificates may not be shared between people.

For Hosts and Services the CN should contain the FQDN of the host. Each DN must have a unique binding to the end entity but this does not preclude an end entity from having multiple certificates with the same DN.

### 3.1.4 Method to Prove Possession of Private Key

Obtaining a personal or individual certificate is initiated by a key generation tag or control which the individual's web browser reads on the CA's user registration web page. Key generation and certificate signing request generation and submission are tied together in a single session, and there is a reasonable presumption of possession of private key in requests originating in web browser functions. Keys generated by other means (such as openssl), whether for persons or services, have separate key generation, csr generation, and submission stages. No proof of possession of private key test is made in these cases. Renewal and revocation functions employ a proof of possession of private key test.

### 3.1.5 Authentication of Individual Identity

The DOE Grids PKI uses an architecture where the approval of certificate requests is the responsibility of the Registration Authority for a specific community. The work flow of subscriber certificates request/approval can be found on the service website: http://www.doegrids.org/pages/workflow.pdf

Each RA will be responsible for determining the identity used in the subject field of the Certificate. The procedure for determining identity differs depending on the type of certificate and RA policies. Each VO/Site must document their procedures in their individual RA appendix in this document.

## *3.2 Routine Rekey*

No Stipulation

## *3.3 Rekey After Revocation*

Rekey after revocation follows the same rules as an initial registration.

## *3.4 Revocation Request*

See section 4.4.2 for details on who can request a certificate revocation.

# 4 Operational Requirements

## 4.1 Certificate Application

Procedures are different if the subject is a person or a host. **In every case the subject has to generate its own key pair.** A Key pair must have a minimum key length of 1024 bits. Requests are submitted by a secure online procedure, Notice of the request is sent to the VO's or Site's RA for validation. (see Appendix A and Appendix for specific RA). Information in the request must comply with Subscriber Obligations specified in Section 2.1.2.

**Person**.
The individual making the request is authenticated according to procedures described elsewhere in this document.

**Host or Service**.
Individuals requesting a service certificate must either have a valid DOEGrids personal certificate, or the requestor will be authenticated as for a Person certificate request.

## 4.2 Certificate Request cancellation

The CA managers will cancel certificate requests that have not been processed in a reasonable time (at least 30 days from submission). The CA managers will periodically send notifications to the RA to inform them about certificate requests that are pending in the CA queue.

The CA managers will revoke certificates whose email address is non functional for 30 days. They will make a best effort attempt to notify the RA when the 1st bounce of the email address occurs.

## 4.3 Certificate Issuance

DOE Grids PKI issues the certificate if, and only if, an RA has validated the identity of the requestor and verified that the requestor is the owner of the DN. A message is sent to the requestor's e-mail address with the instructions on how to download it from the DOE GRIDS PKI web server.

## 4.4 Certificate Acceptance

No Stipulation.

## 4.5 Certificate Suspension and Revocation

### 4.5.1 Circumstances for Revocation

CA operational staff has the authority to revoke any certificate issued by DOEGrids. A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- The subscriber's private key is lost or suspected to be compromised;
- The information in the subscriber's certificate is suspected to be inaccurate;
- The subscriber no longer needs the certificate to access Relying Parties' resources;
- The subscriber violated his/her obligations.

- The ownership of the DN is transferred to a new owner, all valid certificates issued to the previous owner will be revoked.

### 4.5.2 Who Can Request Revocation

A request to revote an End Entity Certificate (Person, Host or Service) can be done by the following entities if they can present reasonable evidence that the private key has been compromised or that the subscriber's data is in error:

- The Holder or owner of the Certificate.
- The RA for the VO or Site that validated the original Certificate request
- The DOE GRIDS PKI managers.
- The DOE Grids Incident response team
- Any other official entity that is a member of the VO or Site.

The subscriber may revoke (or request revocation of) the subscriber's own certificate for any reason at any time.

### 4.5.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself to the DOE GRIDS PKI or the VO's RA staff, which must use the same procedures used for the authentication of identity of a person. The RA that issued the certificate will be notified immediately about the revocation request and will be granted one business day to resolve any uncertainties about the circumstances causing the revocation request, except in cases where the CA managers determine that a revocation grace period will cause damage to relying parties.

### 4.5.4 Circumstances for Suspension

The DOEGrids PKI does not support Certificate Suspension.

### 4.5.5 CRL Issuance Frequency

CRLs are issued after every certificate revocation or refreshed once every month if there are no changes.

### 4.5.6 Online Revocation/status checking availability

An online Status checking facility will be provided as an experimental service.

### 4.5.7 Online Revocation checking requirements

No stipulation.

### 4.5.8 Other forms of revocation advertisement available

No stipulation.

## *4.6 Security Audit Procedures*

Security Auditing of the DOEGrids PKI is not supported.

## *4.7 Records Archival*

### 4.7.1 Types of Event Recorded

The following events are recorded and archived

- Certification requests;

- Revocation requests;
- Issued certificates;
- Issued CRLs;
- All e-mail correspondence on the PMA mailing list;

### 4.7.2 Retention Period for Archives

Minimum retention period is three years.

## *4.8 Key Changeover*

No stipulation.

## *4.9 Compromise and Disaster Recovery*

If the CA's private key is — or suspected to be - compromised, the CA will:

1. Inform subscribers and subordinate RAs;
2. Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

## *4.10 CA Termination*

Before DOE GRIDS PKI terminates its services, it will:

1. Inform subscribers and subordinate RAs;
2. Make widely available information of its termination;
3. Stop issuing certificates and CRLs.
4. Destroy its private key's and all copies.

# 5 Physical, Procedural and Personnel Security Controls

## 5.1 Physical Security Controls

The DOE GRIDS PKI is located at Lawrence Berkeley National Laboratory (LBNL) in the ESnet Data Center. The ESnet Data center maintains a limited access procedure keyed to the LBNL badge system. The servers are maintained in access controlled secure racks. All access to the servers is limited to DOE GRIDS PKI Security officer and system support staff of ESnet. All servers are Sun Solaris systems. Security on these systems is maintained and configured to highest level provided for by Sun. All security patches will be applied as soon as they are released by Sun and verified by the ESnet support staff.

The DOE GRIDS PKI servers are located behind a Cisco Pix Firewall. The entire server farm will be monitored by the Bro intrusion detection system.

## 5.2 Procedural Controls

No Stipulations.

## 5.3 Personnel Security Controls

All access to the servers and applications that comprise the DOE GRIDS PKI is limited to DOE GRIDS PKI Security officer and the ESnet system support staff.

# 6 Technical Security Controls

## *6.1 Key Pair Generation and Installation*

### 6.1.1 Key Pair Generation

Each End Entity must generate its own key pair. DOE GRIDS PKI does not generate private keys.

### 6.1.2 Private Key Delivery to Entity

The DOE GRIDS PKI never has access to the End Entity private key.

### 6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to the issuing CA in a secure and trustworthy manner (e.g. SSL/TLS).

### 6.1.4 CA Public Key Delivery to Users

CA certificate is delivered by an online transaction from a secure web server or by other out of band secure process.

### 6.1.5 Key Sizes

Keys of length less then 1024 bits will not be signed.

### 6.1.6 Public Key Parameters Generation

No stipulation.

### 6.1.7 Parameter Quality Checking

No stipulation.

### 6.1.8 Hardware/Software Key Generation

No Stipulation.

### 6.1.9 Key usage Purposes

DOE GRIDS certificates are only warranted for authentication and signing proxy certificates [Proxy].

The ESnet root CA private key will only be used to sign subordinate CAs. The DOE GRIDS online CA signing key is the only key that will be used for signing CRLS and Certificates for Persons, Services.

The Certificate key Usage field must be used in accordance with [RFC2459]

## *6.2 Private Key Protection*

### 6.2.1 Private Key (n out of m) Multi person control

Not supported.

### 6.2.2 Private Key Escrow

Not supported.

### 6.2.3 Private Key Archival and Backup

There is no support for Private Key Archival and Backup for End Entity Certificates.

## *6.3 Other Aspects of Key Pair Management*

DOE GRIDS CA certificate has a validity of **five** years.

## *6.4 Activation Data*

DOE GRIDS CA private key is protected by a pass phrase.

DOE GRIDS CA signing key is protected by a 3DES key. This key is known only to a set of operator smart cards (the OCS), which are unlocked by pass-phrases individually assigned to each card.

## *6.5 Computer Security Controls*

### 6.5.1 Specific Computer Security Technical Requirements

CA servers include the following:

Operating systems are maintained at a high level of security by applying all recommended and applicable security patches;

Monitoring is done to detect unauthorized software changes;

Services are reduced to the bare minimum;

### 6.5.2 Computer Security Rating

No stipulations.

## *6.6 Life-Cycle Security Controls*

No stipulations.

## *6.7 Network Security Controls*

DOE GRIDS will maintain an Online CA for issuing Certificates authorized by the DOE GRIDS RAs.

The DOE GRIDS PKI servers are located behind a Cisco Pix Firewall. The entire server farm will be monitored by ESnet intrusion detection services.

## *6.8 Cryptographic Module Engineering Controls*

DOE GRIDS CA signing private key is managed by an nCipher FIPS-140 complaint hardware and software system.

This private key is stored in 3DES encrypted form on the hard disk of the server, and is backed up by conventional server backup services and by other means. The private key is never available in plain text form (that is, in a usable form) to the server operating system or any back up service. The private key is managed by a set of smart cards.

The keys for these smart cards, and the 3DES key used to encrypt the signing private key, are generated by the nCipher nShield FIPS 140 device (key generation is based on a hardware random number generator). Access to these keys is only available through a set of administrator smart cards. Several copies of cards have been created and stored in secure locations.

# 7 Certificate and CRL Profiles

## *7.1 Certificate Profile*

### 7.1.1 Version number

X.509 v3.

### 7.1.2 Certificate Extensions

This section must follow the minimum requirements as stated in the 1.1.

**Basic Constraints** (CRITICAL)
not a CA.(default configuration; ASN.1 compiler removes default empty sequences)

**Netscape Certificate Type**

SSL Client (all); SSL Server (host or service); secure email (optional, person)

**Key Usage** (CRITICAL)
Digital Signature, Non Repudiation, Key Encipherment (all); Data Encipherment (service only)

**Authority Key Identifier**

**Subject Alternative Name**
dnsName (service certificates)

RFC822name (DN owner's email address; can be individual or group address)

**CRL Distribution Points**

**Certificate Policies** OID

### 7.1.3 Algorithm Object identifiers

No stipulations.

### 7.1.4 Name Forms

The X.509 character set is case insensitive. But in some situations software being used to interpret these fields does interpret the name forms as case sensitive. To insure proper operation, relying parties must make sure the case used in Globus map files match the case of issued certificates. Until uniform interpretation of case is deployed it is strongly recommended that we follow the case conventions that are used in the examples below.

OU=Hosts, is only for internal use of DOE GRIDS.

**Issuer**: CN=DOE Grids CA 1; OU=Certificate Authorities; DC=doegrids; DC=org

The subject name of the End Entity will be a valid Distinguished Name (DN). These DNs will consist of one of the following Relative DNs (RDN):

- **For People:** OU=People; DC= doegrids; DC=org
- **For Hosts:** OU=Hosts; DC= doegrids; DC=org
- **For Services:** OU=Services; DC= doegrids; DC=org

The Common Name (CN) components of the DNs are defined as:

**For a Person**.
Full name as determined by the RA and an additional 5 random alphanumeric characters added for uniqueness. (i.e. "John K. Doe 1W2D3")

CN= John K. Doe 1W2D3; OU=People; DC= doegrids; DC=org

**For a Host**.
A fully qualified Domain name as registered in DNS or its 4 octet IP address, optionally prefixed with "host/".

CN= george.lbl.gov; OU=Hosts; DC= doegrids; DC=org

**For a Service**.
The Service name/A fully qualified Domain name as registered in DNS (FQDN) or its 4 octet IP address (i.e.<SRV>/<FQDN>;<SRV>/<IP> ) note: “host” is an acceptable service name, as for example in Globus gatekeeper certificates.

- CN= FTP/george.lbl.gov; OU=Services; DC= doegrids; DC=org
- CN= FTP/131.243.2.12; OU=Services; DC= doegrids; DC=org
- CN= george.lbl.gov; OU=Services; DC= doegrids; DC=org

### 7.1.5 Name Constraints

Not supported

### 7.1.6 Certificate Policy Object Identifier

OID: [ESnet].ERmember.DOEGrids.CP-CPS.CPVersionNumber.CPReleaseNumber

1.2.840.113612.3.7.1.2.10

### 7.1.7 Usage of Policy Constraints Extensions

No stipulation.

### 7.1.8 Policy qualifier syntax and semantics

The qualifier is a pointer to this document, in the form of an URL.

## *7.2 CRL Profile*

### 7.2.1 Version

X.509 v2

### 7.2.2 CRL and CRL Entry Extensions

The CRL is using version 2 extensions for the CRL and entries. It will contain the CRL number, Critical, and Number. The CRL extension example:

Extensions:
Identifier: CRL Number - 2.5.29.20
Critical: no
Number: 412

The individual entry on the CRL will include: Serial Number, Revocation Date, Revocation Reason and Invalidity Date. Invalidity Date is the date the relying party should consider the certificate was no longer valid. This date maybe earlier then the revocation date. The following is an example of an entry on the DOEGrids CRL:

Serial Number: 0x58D – of the certificate

Revocation Date: Wednesday, January 21, 2004 3:56:10 PM PST

Extensions:

Identifier: Revocation Reason - 2.5.29.21

Critical: no

Reason: Superseded
Identifier: Invalidity Date - 2.5.29.24
Critical: no
Invalidity Date: Wed Jan 21 00:00:00 PST 2004

# 8 Specification Administration

## 8.1 Specification Change Procedures

Users will not be warned in advance of changes to DOE GRIDS CA's policy and CPS.

## 8.2 Publication and Notification Procedures

The policy is available at:

http://www.doegrids.org/CA/DOEGrids%20CA%201/Certificate%20Policy.pdf

## 8.3 CPS Approval Procedures

The DOE GRIDS PKI PMA is responsible for the CP and CPS. All changes must be approved by the PMA.

# Appendix A: General Guidelines for DOEGrids Registration Authorities, Agents and Grid Admins

## A.1 Background

This set of guidelines is intended to address in general how Registration Authorities and their Agents will operate. Specific RA and Agent instructions for member VOs and sites are covered by their member Appendix in this CP/CPS.

The DOEGrids PKI is managed by the DOEGrids Policy Management Authority. This PMA consists of DOEGrids PKI Registration Authorities or their designated Point of Contact, community experts, PKI operations staff and ex official members.

DOEGrids Operations (DOEGrids-CA-1@DOEGrids.org) will be responsible for the verification of RA and/or their Agents certificates used to approve/reject/revoke certificates. Also, to insure that the RA or Agent is aware of their duties letters acknowledging the person's role and responsibilities must be sent to DOEGrids Operations. Examples of these letters are included in this appendix. DOEGrids Operations require that these letters be digitally signed and mailed to DOEGrids Operations. The signed email will be used to verify the possession of the private key and will convey to DOEGrids Operations the certificate that will be used in the new or renewed role. If the applicant can not send digitally signed email, DOEGrids operations will use another equally trusted method to verify proof of possession of the private key for the certificate to be used in the new role. The letter can be physically signed and faxed to DOEGrids Operations.

Non-DOEGrids certificates can be used in RA and Agent roles. If non-DOEGrids certificates are used, they must be part of the IGTF or be of equivalent or higher quality than DOEGrids.

## A.2 Guidelines

- Registration Authorities (RA) or their designated Registration Agents (RAg) will perform all of the functions needed to apply certificate issuance policy to potential CA subscribers.
- The RA for each site/VO designates a Point of Contact who becomes a member of the DOEGrids PMA as the voting representative of the site/VO.
- Each RA must sign a DOEGrids RA agreement. This Agreement (§ A.3.1) must be sent to DOEGrids Operations as a digitally signed email and resubmitted annually during the renewal of the RA's personal certificate. The certificate used to digitally sign the email to DOEGrids Operations will be used to authorize the RA to approve/revoke certificates.
- A DOEGrids RA can appoint one or more Registration Agents. These agents do not need the approval of the DOEGrids PMA.
- Each RA that wishes to appoint an Agent must send a digitally signed email (§ A.3.2) to DOEGrids Operations identifying the person to be an Agent. This email must be resubmitted annually during the renewal process of the Agents personal certificate.
- Each Agent of an RA must sign a DOEGrids Agent Agreement. This agreement (§ A.3.3) must be sent to the DOEGrids Operations as a digitally signed email and resubmitted annually during the renewal of the Agents personal certificate. The certificate used to digitally sign the email to DOEGrids Operations will be used to authorize the Agent to approve/revoke certificates.
- The Agents appointed by the VO/Site shall have a term of one year and must be recertified by the RA in this role during the annual renewal of their Agent certificates.
- The RA or their Agent must check if the requested DN in the certificate request is new and unique and, if so, continues to process request. If the DN already exists the RA/Agent must verify that the requester is the registered owner of the DN and,

if so, continues to process the request. If requestor is not the registered owner of the DN the RA/Agent either handles a transfer of ownership for the DN or rejects the request. In case of transfer of ownership, all previous certificates with the same DN will be revoked.

- The RAs and RAg needs to be technically qualified and have the organizational authority to make the decision on whether the organization will issue a certificate to an applying individual (or to hosts on behalf of an individual that already has an DOEGrids signed certificate).
- RAs and their Agents, by policy **MAY NOT** do the following:
  1. Sign CA certificates.
  2. Sign a name space not approved by this policy.
  3. Sign a name space for a Service certificate that is not part of their VO/site.

## *A.3 Agreements for Registration Authority, Agents and Grid Admins*

Each of these named roles in the DOEGrids PKI - Registration Authority, Agent, and Grid Admin – must send a digitally signed email to their respective authority. This digitally signed email will be the formal acknowledgement of their responsibilities and roles as a DOEGrids RA, Agent or Grid Admin. This email must be presented and accepted by the responsible authority before the RA, Agent or Grid Admin certificate is authorized to approve or revoke DOEGrids certificates.

The following four email templates are provide for convenience. They are included in the sections that follow.

1. RA Declaration to DOEGrids PMA
   This letter must be sent as a signed email to the DOEGrids PMA. It should be sent to: doegrids-ca-1@doegrids.org
2. Letter requesting assignment of RA Agent Role
   This letter is from an RA to the DOEGrids CA operations asserting that a person has been assigned an Agent role. This letter must be sent as a signed email to the DOEGrids CA operations. It should be sent to: doegrids-ca-1@doegrids.org
3. Letter requesting RA Agent role
   This letter must be sent as a signed email to the DOEGrids CA operations. It should be sent to: doegrids-ca-1@doegrids.org
4. Letter requesting Grid Admin Role
   This letter is written by the individual requesting to be a Grid Admin and sent to the responsible Registration Authority.

### A.3.1 RA declaration to DOEGrids PMA

Dear DOEGrids PMA:

I [*Name*] will be acting as the Registration Authority for [*VO/Site*]. I have been authorized by my [*VO/Site*] to represent them for the purposes of approving/revoking DOEGrids certificates in our community. I appoint [*Name*] to be the Point of Contact for [*VO/Site*] and our voting member on the DOEGrids PMA. I have read and agree to the following clauses:

1. In acting as the RA for [VO/Site] I have read, understood and accept the responsibilities and tasks assigned to a RA as laid out in the DOEGrids CP/CPS. http://www.doegrids.org/Docs/CP-CPS.pdf.
2. I understand that DOEGrids Certification Service will notify me by email of changes to CP/CPS and I will immediately notify the DOEGrids PMA if I am no longer willing to act as a RA under any new CP/CPS.

3. I understand that failure to fulfill my responsibilities and tasks under this agreement may result in the termination of my appointment as a RA.
4. I agree only to act on enrolment requests associated with the [VO/Site].
5. I understand that I am responsible for the revocation of certificates that are suspected of being compromised or issued in violation of the DOEGrids CP/CPS policies or requested by the owner.
6. I understand that I am responsible for all customer support for our [VO/site] related to DOEGrids certificate issuance, revocation and information.

### A.3.2 Letter requesting assignment of RA Agent Role

Dear DOEGrids Operations:

I [*Name*] as the Registration Authority for [*VO/Site*] would like to appoint [*Name*] to be an RA Agent for my [*VO/Site*]. He/she will represent our community for the purposes of approving/revoking DOEGrids certificates in our community. I have read and agree to the following clauses:

The new Agent [Name], [email address] is familiar with the contents of the DOEGrids CP/CPS, the [VO/Site] authentication procedures, and agent duties as described in CPS.

I agree that I am responsible for the actions of [Name, Email address] in his/her role as Agent.

### A.3.3 Letter requesting RA Agent Role

Dear DOEGrids Operations:

I [*Name*] will be acting as an Agent of the Registration Authority for [*VO/Site*]. I have been authorized by my [*VO/Site*] to represent them for the purposes of approving/revoking DOEGrids certificates in our community. I have read and agree to the following clauses:

1. In acting as the Agent of the RA for [VO/Site] I have read, understood and accept the responsibilities and tasks assigned to an Agent as laid out in the DOEGrids CP/CPS. http://www.doegrids.org/Docs/CP-CPS.pdf.
2. I understand that DOEGrids Certification Service will notify me by email of changes to CP/CPS and I will immediately notify the DOEGrids PMA if I am no longer willing to act as an Agent for my RA under any new CP/CPS.
3. I understand that failure to fulfill my responsibilities and tasks under this agreement may result in the termination of my appointment as a Agent for [VO/Site]
4. I agree only to act on enrolment requests associated with the [VO/Site].
5. I understand that I am responsible for the revocation of certificates that are suspected of being compromised or issued in violation of the DOEGrids CP/CPS policies.
6. I understand that I am responsible for customer support for our [VO/site] related to DOEGrids certificate issuance, revocation and information.

### A.3.4 Grid Admins

A DOEGrids RA can appoint one or more Grid Admins to serve their community. These agents do not need the approval of the DOEGrids PMA. The Grid Admin is a special assigned role in the DOEGrids PKI that allows special DOEGrids Agents the ability to submit and approve certificates for Grid Services. This role is not authorized to issue People certificates.

The purpose of this role is to help minimize the work load of system administers that manage large numbers of Grid hosts and services.

These Agents or Grid Admins do not have all the privileges of regular Agents. They can only submit requests for service certificates in a namespace as specified by the appointing RA. They can request and approve service certificates for this namespace only.

The following documents describe how to set up and use the Grid Admin role:

http://www.doegrids.org/Library/CMS47/Grid_Admin_Interface_v1.0-Agent_Guide.doc
http://www.doegrids.org/Library/CMS47/Grid_Admin_Interface_v1.0-User_Guide.doc

### A.3.4.1 Letter Requesting a Grid Admin role

This letter is written by the individual requesting to be a Grid Admin and sent to the responsible Registration Authority.

Dear RA of VO/Site:

I [*Name of new Grid Admin*] would like to be a Grid admin for [*VO/Site*]. I would like to be authorized to request and approve DOEGrids Service certificates for the following name space(s):

a. FQDN 1 or range of addresses for a particular domain
b. FQDN 2
c. others

1. As the Grid Admin for [VO/Site] I have read and understand the responsibilities and tasks assigned to a Grid Admin as laid out in the DOEGrids CP/CPS. http://www.doegrids.org/Docs/CP-CPS.pdf.
2. I agree that as Grid Admin I will only submit and approve Service certificates for the FQDNs listed above.
3. I understand that I am responsible for the revocation of certificates that are suspected of being compromised or issued in violation of the DOEGrids CP/CPS policies

# Appendix B: PPDG RA operational procedure

The PPDG RA will stop issuing new certificates as of Sept. 1, 2006.All continuing obligations of the PPDG RA, including records retention and certificate revocation, are assumed by the OSG RA.

## *B.1* Background

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOE GRIDS CA is the Particle Physics Data Grid Registration Authority (PPDG RA). Information defining the PPDG VO is available at http://www.ppdg.net/. This appendix describes how the responsibilities for a VO RA are implemented for the PPDG RA.

It is expected that the PPDG RA will have a finite lifetime and is implemented an example of a VO RA which can serve the needs of the PPDG community until other persistent RA's are developed which serve this community***PPDG RA staff***

### B.2.1 Membership

A number of persons are identified as comprising the PPDG RA staff. This list of persons is openly available on the PPDG RA web site (http://www.ppdg.net/RA/sponsors.htm). Each of these persons has a valid certificate from the DOE GRIDS CA.

The initial set of persons to be included in the PPDG RA staff is the PPDG Steering Committee. Additional persons may be appointed to the PPDG RA staff by the PPDG steering committee and approved by the DOE GRIDS CA.

### B.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the <VO> about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for the <VO>. The POC shall be a member of the DOE GRIDS CA PMA.

## *B.3 PPDG VO Community*

The PPDG Virtual Organization community is defined as all persons who are member of or collaborating with the Computer Science groups and Physics Experiments participating in PPDG. These CS groups and physics experiments are listed at http://www.ppdg.net/. The privilege of requesting a certificate is subject to restrictions defined in this document.

## *B.4 Authentication procedures*

### B.4.1 Authentication of individual identity

Any member of the PPDG RA staff may authenticate a person to satisfy a request from the POC. Person requesting certification must demonstrate reasonable evidence of membership in the PPDG VO

### B.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between PPDG RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.

The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- face-to-face conversation
- telephone conversation between members of PPDG RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- secure digitally signed email between individuals with certificates from DOE GRIDS CA.

### B.4.3 Steps in authentication for certification

### B.4.3.1 Person Certificate

1. A person requests a certificate from the DOE GRIDS CA community RM.
2. Agent receives notification of request and takes assignment if appropriate for this RA.
3. Agent contracts sponsor from predefined list PPDG RA staff members.
4. PPDG RA staff confirms or refutes request to Agent.
5. Agent approves or rejects request using community RM.
6. Person requesting certificate receives notification from RM.

### B.4.3.2 Host or Service Certificate

1. A person requests a host or servcie certificate from the DOE GRIDS CA community RM.
2. Agent receives notification of request and takes assignment if appropriate for this RA.
3. Agent checks if person has a valid DOE GRIDS CA certifiate.
4. Agent checks if the DN is new and unique and, if so, continues to process request. If DN already exists agent verifies that requester is registered owner of the DN and, if so, continues to process the request. If requestor is not the registered owner of the DN the agent either handles a transfer of ownership for the DN or rejects the request. In case of transfer of ownership, all previous certificates with the same DN will be revoked.
5. Agent approves request if person has a valid DOE GRIDS certificate and rejects request if person does not have a valid DOE GRIDS certificate.

## *B.5 Lifetime of certificates*

Identity certificates approved by the PPDG RA have a lifetime of no more than 12 months from date of approval.

# Appendix C: National Fusion Collaboratory's RA operational Procedures

## *C.1 Purpose, Goals, Scope*

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOE GRIDS CA is the National Fusion Collaboratory Registration Authority (NFC RA). Information defining the National Fusion Collaboratory is available at http://www.fusiongrid.org/. This appendix describes how the responsibilities for a VO RA are implemented for the NFC RA.

The National Fusion Collaboratory is a creation of a SciDAC proposal to "advance the science of high temperature plasma physics for magnetic fusion". This VO will exist for at least the 3-year funding period of that proposal, and if successful may become a more lasting entity. The need for the NFC RA itself will last as long as the Collaboratory does, and will at least cover the period where any X.509 certificates approved by this RA are still valid.

## *C.2 NFC RA staff (sponsors)*

### C.2.1 Membership

A number of persons are identified as comprising the NFC RA staff, which is the group of sponsors who are authorized to perform the identity check on individuals requesting a certificate. This list of persons is available to NFC members at (www.fusiongrid.org/Security). Each of these persons has a valid certificate from the DOE GRIDS CA.

The initial set of persons to be included in the NFC RA staff is comprised of the PI s from each of the 6 institutions funded by the National Fusion Collaboratory SciDAC project. Additional persons may be appointed to the NFC RA staff by the current members with the approval of the DOE GRIDS CA.

### C.2.2 Point of Contact (POC) with DOE GRIDS CA (agent)

All necessary communications between the DOE GRIDS CA and the NFC about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for the NFC. The POC shall be a member of the DOE GRIDS CA PMA.

## *C.3 NFC VO Community*

The NFC Virtual Organization community is defined as all persons authorized to use any of the National Fusion Collaboratory's on-line resources. Any one of the Collaboratory PI's may authorize a new member of the community. The privilege of requesting a certificate is subject to restrictions defined in this document.

## *C.4 Authentication procedures*

### C.4.1 Authentication of individual identity

Any member of the NFC RA staff (a sponsor) may authenticate a person requesting a certificate. Person requesting certification must demonstrate reasonable evidence of membership in the NFC VO.

### C.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between NFC RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.

The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- face-to-face conversation
- telephone conversation between members of NFC RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- secure digitally signed email between individuals with certificates from DOE GRIDS CA.

### C.4.3 Steps in authentication for certification

### C.4.3.1 Person Certificate

1. A person requests a certificate from DOE GRIDS CA community RM; the request includes the name of a NFC RA staff (sponsor) that can authenticate the request.

2. Agent receives notification of the request and takes assignment if appropriate for this RA.

3. Agent notifies NFC RA sponsor indicated in request that a request is pending including the name, institution and email of the requester

4. NFC RA sponsor contacts requester and authenticates request (secure means).

5. NFC RA sponsor confirms or refutes the request to the agent. (secure means)

6. Agent approves or rejects the request using the community RM.

7. Person requesting certificate receives notification from RM.

### C.4.3.2 Host or Service Certificate

1. A person requests a host or service certificate from the DOE GRIDS CA community RM.
2. Agent receives notification of the request and takes assignment if appropriate for this RA.

3. Agent verifies that requesting person has a valid DOE GRIDS certificate.
4. Agent checks if the DN is new and unique and, if so, continues to process request. If DN already exists agent verifies that requester is registered owner of the DN and, if so, continues to process the request. If requestor is not the registered owner of the DN the

agent either handles a transfer of ownership for the DN or rejects the request. In case of transfer of ownership, all previous certificates with the same DN will be revoked.
5. Agent approves the request if the requester has been designated by a NFC sponsor to receive host or service certificates for the site specified in the certificate host name.
6. Person requesting the certificate receives notification from the RM.

## *C.5 Lifetime of certificates*

Identity certificates approved by the NFC RA have a lifetime of no more than 12 months from date of approval.

# Appendix D: NERSC RA operational procedures

## *D.1 Background*

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOE GRIDS CA is the National Energy Research Scientific Computing Center (NERSC) Registration Authority (NERSC RA). Information defining the NERSC VO is available at http://www.nersc.gov/. This appendix describes how the responsibilities for a VO RA are implemented for the NERSC RA.

NERSC is the Department of Energy's largest unclassified high performance computing center. Its primary mission is to accelerate the pace of scientific discovery in the DOE Office of Science community by providing high-performance computing, information, and communications services. NERSC's client base is global in scope and many DOE projects and collaboration utilize NERSC's resources for their computational needs. The need for the NERSC RA is permanent for the foreseeable future and will eventually be the primary authentication and authorization mechanism for access to NERSC resources.

## *D.2 NERSC RA staff*

### D.2.1 Membership

A number of persons are identified as comprising the NERSC RA staff. These persons have been designated by NERSC and are NERSC staff members. Each of these persons has a valid certificate from the DOE GRIDS CA.

The initial set of persons to be included in the NERSC RA staff are responsible for implementing and ensuring the NERSC RA complies with both DOE GRIDS CA guidelines and also pre-existing NERSC authentication and authorization mechanisms.

### D.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the NERSC VO about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for the NERSC VO. The POC shall be a member of the DOE GRIDS CA PMA.

Communication with the NERSC RA on operational issues should be via the email address certs@nersc.gov. This address will forward mail to the NERSC POC,

## *D.3 NERSC VO Community*

The NERSC Virtual Organization community is defined as all persons who are authorized to utilize NERSC resources. The privilege of requesting a certificate is subject to restrictions defined in this document.

Note that there may be some overlap between the NERSC VO Community and the OSG Community (Appendix N). While the NERSC RA is primarily responsible for NERSC usage, the OSG RA may also issue certificates to these users, in some cases. In these cases, the certificates would be subject to the OSG operational procedures and policies defined in Appendix N.

## *D.4 Authentication procedures*

### D.4.1 Authentication of individual identity

Authentication of an individual identity must follow existing NERSC guidelines for client authentication. Persons requesting certification must demonstrate reasonable evidence of membership in the NERSC VO. All individuals must contact NERSC account support for authentication. The NERSC account support staff will contact the NERSC RA POC regarding the results of the authentication procedure.

### D.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between NERSC RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information. The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- Face to face conversation.
- Telephone conversation between members of NERSC RA staff.
- Telephone conversation between members of NERSC RA staff and NERSC VO users at telephone number listed in institutional phone book. User is authenticated by NERSC RA staff based on information stored in the NERSC Information Management (NIM) database.
- Secure digitally signed email between individuals with certificates from DOE GRIDS CA.
- Paper documents physically signed and dated by either NERSC RA staff or DOE GRIDS CA staff

Note that face to face communication may not always be feasible, because NERSC operates as a “catch-all” RA, and includes geographically distributed users. In this case, user verification is based on information obtained from out of band communication during the initial NERSC account allocation process. This includes:

- A signed hard copy of the NERSC Computer Use Policy Form, with the following information:
  - Name
  - Citizenship
  - Organization
  - Email Address
  - Work Phone Number
  - Principal Investigator

  This form can be found at: http://www.nersc.gov/nusers/accounts/usage.php,

- Institutional information.
- P.I. approval.

- Verification of user information via telephone communication.

This information is subsequently stored in the NIM database.

All instances of communication essential for authenticating individual entities will be logged and archived by NERSC RA staff. This archive will only be accessible to NERSC RA staff and other authorized agents and will contain the date and time of the communication, names of the parties involved in the communication, name of individual the communication is in regards to and any other pertinent information that would be deemed essential to reconstruct the communication if so required.

### D.4.3 Steps in authentication for certification

1. Individual requests a certificate from DOE GRIDS CA, the request includes the name of NERSC VO who will authenticate the request. (secure means)
2. DOE GRIDS CA notifies NERSC RA POC and NERSC RA staff of a certification request. (insecure means)
3. NERSC RA Staff retrieves information of certification request from DOE GRIDS CA (secure means).
4. NERSC RA staff member looks up requestor contact information in the NERSC Information Management (NIM) database. This will be used for establishing a secure means to authenticate the user. Requestor MUST be an existing NERSC user, with an existing account in the NIM database.
5. NERSC RA staff member contacts requestor via secure channel and authenticates individual per existing NERSC authentication policy and mechanisms. (secure means)
6. NERSC RA staff member logs the communication used to authenticate the requestor, as described in this document.
7. NERSC RA staff member notifies NERSC POC that authentication has occurred (insecure means)
8. POC calls NERSC RA staff at telephone number listed in institutional phone book, and verifies status of authentication (secure means)
9. POC or NERSC RA Staff notifies DOE GRIDS CA of the authentication of the request (secure means)

The above procedure only applies to authentication for existing members of the NERSC VO. NERSC will not issue certificates to a requestor that does not have an existing NERSC account. Please refer to http://www.nersc.gov/nusers/accounts/get.php for information on how NERSC user accounts may be obtained. Initial user verification during the allocation process is described in D.4.2.

## *D.5 Lifetime of certificates*

Identity certificates approved by the NERSC RA have a lifetime of no more than 12 months from date of approval.

# Appendix E: Lawrence Berkeley Lab's RA operational Procedures

## *E.1 Purpose, Goals and Scope*

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOE GRIDS CA is the Lawrence Berkeley National Laboratory Registration Authority (LBNL RA). Information defining the LBNL site is available at http://www-itg.lbl.gov/gtg. This appendix describes how the responsibilities for a VO RA are implemented for the LBNL RA. The need for the LBNL RA will probably span the lifetime of the DOE GRIDS itself.

## *E.2 VO RA staff*

### E.2.1 Membership

A number of persons are identified as comprising the LBNL RA staff, which is the group of sponsors who are authorized to perform the identity check on individuals requesting a certificate. This list of persons is openly available on the LBNL Grid Technologies Group web site (http://www-itg.lbl.gov/gtg). Each of these persons has a valid certificate from the DOE GRIDS CA. Additional persons may be appointed to the LBNL RA staff by its current members with the approval of the DOE GRIDS CA.

### E.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the <VO> about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for the <VO>. The POC shall be a member of the DOE GRIDS CA PMA.

## *E.3 LBNL Site Community*

The LBNL site community is defined as all persons authorized to use any of the LBNL grid resources. The privilege of requesting a certificate is subject to restrictions defined in this document.

## *E.4 Authentication procedures*

### E.4.1 Authentication of individual identity

Any member of the LBNL RA staff (a sponsor) may authenticate a person to satisfy a request from the POC. Person requesting certification must demonstrate reasonable evidence of participation in DOE GRIDS activities.

### E.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between LBNL RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.
The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- face-to-face conversation
- telephone conversation between members of LBNL RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- Secure digitally signed email between individuals with certificates from DOE GRIDS CA.

### E.4.3 Steps in Authentication for Certification

1. A person requests a certificate from DOE GRIDS CA, the request includes the name of a LBNL RA staff who can authenticate the request. (secure means)
2. DOE GRIDS CA notifies LBNL RA POC of a certification request. (insecure means)
3. POC retrieves information of certification request from DOE GRIDS CA (secure means).
4. POC notifies LBNL RA staff member indicated in request that a request is pending including the name, institution and email of the requester (insecure means)
5. LBNL RA staff contacts requester and authenticates request by means specified in this document.
6. LBNL RA staff notifies POC that authentication has occurred (insecure means)
7. POC calls LBNL RA staff at telephone number listed in institutional phone book, and verifies status of authentication (secure means)
8. POC notifies DOE GRIDS CA of the authentication of the request (secure means)

## *E.5 Lifetime of certificates*

Identity certificates approved by the PPDG RA have a lifetime of no more than 12 months from date of approval

# Appendix F: ORNL RA operational procedures

## *F.1 Background*

The Oak Ridge National Laboratory (ORNL) Registration Authority (RA) is one of the RAs operating with delegated authority of the DOE GRIDS CA. The laboratory is defined at http://www.ornl.gov . This appendix describes how the responsibilities for ORNL RA are implemented at ORNL.

ORNL is a multiprogram science and technology laboratory managed for the U.S. Department of Energy by UT-Battelle, LLC. Scientists and engineers at ORNL conduct basic and applied research and development to create scientific knowledge and technological solutions that strengthen the nation's leadership in key areas of science; increase the availability of clean, abundant energy; restore and protect the environment; and contribute to national security.

The ORNL RA process is subject to review by local account and resource management authorities during its initial implementation and, if successful, it may become an official authentication mechanism for access to ORNL resources.

## *F.2 ORNL RA staff*

### F.2.1 Membership

A number of persons are identified as comprising the ORNL RA staff. These persons have been designated by ORNL and are ORNL staff members. Each of these persons has a valid certificate from the DOE GRIDS CA.

The initial set of persons to be included in the ORNL RA staff are responsible for implementing and ensuring the ORNL RA complies with both DOE GRIDS CA guidelines and existing ORNL authentication and authorization mechanisms. Additional persons may be appointed to the DOE GRIDS RA staff by ORNL and approved by the DOE GRIDS CA PMA. ORNL reserves the right to relieve ORNL RA duties from any of its staff member at any time.

### F.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and ORNL about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for ORNL. The POC shall be a member of the DOE GRIDS CA PMA.

## *F.3 ORNL Community*

The ORNL community is defined as the staff and affiliates of Oak Ridge National Laboratory. Staff is defined as ORNL employees. Affiliates are individuals that are affirmed by ORNL staff as collaborators engaged with on-site activities at ORNL or users of ORNL site facilities. These persons must also be officially authorized to utilize ORNL on-site resources and abide by the most recent ORNL general resource usage policies. The privilege of requesting a certificate is subject to restrictions defined in this document.

## *F.4 Authentication procedures*

### F.4.1 Authentication of individual identity

ORNL staff member will be identified by inspection of their badge. Inspection may take place in person by RA staff members or be conducted by a third party intermediary known and trusted by the RA staff. Trust is based on prior operational interaction with the RA staff.

The affiliate will be identified by a confirmation statement made by collaborating ORNL staff member, which affirms the affiliate's membership in the ORNL community and verifies the association with the affiliate. The staff member will be identified as detailed above.

ORNL staff members and affiliates requesting certificates are required to have valid ORNL user IDs and either on-site computer accounts or official authorizations to use ORNL site facilities.

### F.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between ORNL RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information. The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- Face-to-face conversation
- Telephone conversation between members of ORNL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed email between individuals with certificates from DOE GRIDS CA
- Paper documents physically signed and dated by either ORNL RA staff or DOE GRIDS CA staff

Note that all kinds of conversation (the first three secure communications above) must be supplemented by emails for logging purposes.

All instances of communication essential for authenticating individual entities will be logged and archived by ORNL RA staff. This archive will only be accessible to ORNL RA staff and other authorized agents and will contain the date and time of the communication, names of the parties involved in the communication, name of individual the communication is in regards to and any other pertinent information that would be deemed essential to reconstruct the communication if so required.

### F.4.3 Steps in authentication for certification

## F.4.3.1 Personal Certificate

1. Individual requests a client certificate from DOE GRIDS CA. The request includes the requestor's work email address and, in the case of an affiliate, the name of sponsor who is an ORNL staff member and will claim the requestor as a collaborator or user. (secure means)
2. DOE GRIDS CA notifies ORNL RA of a certification request. (insecure means)
3. ORNL RA staff retrieves information of certificate request from DOE GRIDS CA. (secure means)
4. ORNL RA staff informs requestor the requirements for possessing ORNL user ID and either an on-site computer account or an official user authorization. Requestor needs to apply for them if not already has.
5. The ORNL account and/or resource management staff will review the application and make decision based on existing ORNL authentication and authorization policies.
6. The requestor has to inform ORNL RA staff the system administrators who are responsible for the ORNL user ID/account creation. The requestor also needs to list his/her affiliated project, name of the project PI, and gives a general description of work being performed.
7. ORNL RA staff contacts the PI (or ORNL sponsor in the case of an affiliate) and the system administrators to verify the requestor's identity.
8. If the requestor is successfully vetted, ORNL RA staff approves the certificate request. (secure means)

## F.4.3.2 Host or Service Certificate

1. A person requests a host or service certificate from the DOE GRIDS CA.
2. DOE GRIDS CA notifies ORNL RA of a certification request. (insecure means) .
3. ORNL RA staff retrieves information of certificate request from DOE GRIDS CA. (secure means)
4. ORNL RA checks if the requested host or service CN specifies a FQDN located at ORNL site. (secure means)
5. ORNL RA checks if the person has a valid DOE GRIDS CA certificate and verifies his/her right to have a host or service certificate.
6. ORNL RA approves the request if all the conditions listed above are met and rejects the request otherwise. (secure means)

## *F.5 Lifetime of certificates*

Identity certificates approved by the ORNL RA have a lifetime of no more than 12 months from date of approval

# Appendix G: ANL RA operational procedures

## G.1 Background

The Argonne National Laboratory (ANL) DOEGrids RA is intended to serve the staff and collaborators of the Laboratory. The Laboratory is defined at http://www.anl.gov. This appendix describes how the responsibilities for ANL RA are implemented at ANL.

Argonne National Laboratory is a major multiprogram laboratory managed and operated for the U.S. Department of Energy (DOE) by the University of Chicago under a performance-based contract.

Argonne's mission is to serve DOE by advancing the frontiers of knowledge, by creating and operating forefront scientific user facilities, and by providing innovative and effective tools and solutions for energy and environmental challenges to national and global well-being, in the near and long term, as a contributing member of the DOE Laboratory system.

Argonne supports DOE's missions in science, energy resources, environmental stewardship, and national security, with lead roles in science, operation of scientific facilities, and energy. In accomplishing its mission, Argonne partners with DOE, other federal laboratories, the academic community, and the private sector.

The Argonne RA is subjected to review by local account and resource management authorities.

In addition to the DOEGrids CA, Argonne National Laboratory is a participant in the

- Department of Energy's Entrust Public Key Infrastructure (http://www.cio.energy.gov/cybersecurity/pki.htm)
- General Services Administrations Shared Service Provider (SSP) Public Key Infrastructure established to support Homeland Security Presidential Directive 12 (HSPD-12) (http://www.fedidcard.gov/), as well as
- Its own in-house Argonne National Laboratory Windows Domain Certificate Authority.

Argonne utilizes the features of all of these public key infrastructures, often in combination to study public key technology or to provide new business solutions. Argonne may request that DOEGrids trust a certificates from these other certificate providers. DOEGrids reliance on other certificate providers will be re-evaluated periodically (at least annually).

## G.2 ANL RA staff

### G.2.1 Membership

Argonne National Laboratory's Registration Authority staff will serve as the Registration Authority staff for the Laboratory in support of Argonne's participation in the DOEGrids. These persons have been designated by ANL and are ANL staff members.

The ANL RA staff is responsible for implementing and ensuring the ANL RA complies with both DOEGrids CA guidelines and existing ANL authentication and authorization mechanisms. Additional persons may be appointed to the DOEGrids RA staff by ANL.

The Argonne RA will take responsibility for acting as a proxy for the agents' ordinary renewal agreements.

### G.2.2 Point of Contact (POC) with DOEGrids CA

All necessary communications between the DOEGrids CA and the ANL about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for ANL. The POC shall be a member of the DOEGrids CA PMA.

### G.2.3 Authentication to DOEGrids CA

Argonne National Laboratory RA staff will use their Argonne issued smart cards and accompanying certificates for authentication to the DOEGrids CA. Relying on existing credential reduces the staff's burden of credential management. These certificates are documented in the Certificate Policy Statement entitled *Argonne National Laboratory Windows Domain Certificate Policy Version 1.2 (*https://credentials.anl.gov/CertificatePolicy/rootcp.pdf).

The Argonne National Laboratory Windows Domain Certificate Authority is based on the Enterprise version of Microsoft Certificate Services 2003. Argonne's Microsoft Enterprise Certificate Server is intimately linked with Argonne's central Active Directory service: the Laboratory's central authentication service. Certificates issued by Argonne's Windows Domain Certificate Authority are equivalent to userids and passwords issued by Argonne's central Active Directory service. Argonne's central authentication service has a FIPS-199 rating of (Moderate, Moderate, Moderate).

The Argonne National Laboratory Windows Domain Certificate Authority is approved to operate under an Authority to Operate letter issued by Ronald J. Lutha Site Manager, Department of Energy Argonne Site Office March 28, 2008.

Additionally, Argonne completed a Security Test and Evaluation conducted by Grant Thornton LLP in July 2007. This is the summary statement from Grant Thornton:

> *Based on Grant Thornton's evaluation, the overall security posture for the GCE appears to be effective. Although there remains room for improvement in the area of change management, documentation, and auditing, the existing deficiencies appear to represent low risk to ANL.*

### G.2.4 Communication with DOEGrids CA

Argonne Registration Authority staff will use DOE Entrust (Federal) certificates that have been verified by DOEGrids operations for S/MIME applications. The FIPS-199 rating of the DOE Entrust CA is (Moderate, Moderate, Moderate).

## *G.3 ANL Community*

The ANL RA will serve the staff and affiliates of Argonne National Laboratory.

- Staff is defined as employees of the Laboratory.
- Affiliates are those individuals that are affirmed as collaborators by Argonne staff.

## *G.4 Authentication procedures*

### G.4.1 Authentication of individual identity

Argonne National Laboratory staff member will be identified by inspection of their badge. Inspection may take place in person by RA staff members or be conducted by a third party intermediary known and trusted by the RA staff. Trust is based on prior operational interaction with the RA staff.

Affiliates will be identified based on an affirmation by an ANL staff member. The staff member will identified as detailed above.

### G.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between ANL RA staff to the DOEGrids CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information. The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOEGrids CA.

The means of secure communications acceptable are:

- Face-to-face conversation
- Telephone conversation between members of ANL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed email between individuals with certificates from DOEGrids CA
- Paper documents physically signed and dated by either ANL RA staff or DOEGrids CA staff

### G.4.3 Steps in authentication for certification

1. Individual requests a certificate from DOEGrids CA. In the case of an affiliate the request includes the name of ANL staff member who will claim the subscriber as a collaborator. (secure means)
2. DOEGrids CA notifies ANL RA of a certification request including the name, institution and email of the requester. (insecure means)
3. ANL RA retrieves information of certification request from DOEGrids CA (secure means).
   3.1. ANL RA staff verifies the requestor's identity.
4. If the subscriber is successfully vetted, ANL RA staff approves certificate request (secure means).

## *G.5 Lifetime of certificates*

Certificates will be valid for one year from date of issuance.

# Appendix H: PNNL RA operational procedures

## *H.1 Background*

The Pacific Northwest National Laboratory (PNNL) DOE GRIDS RA is intended to serve the staff and collaborators of the Laboratory. The Laboratory is defined at http://www.pnl.gov. This appendix describes how the responsibilities for PNNL RA are implemented at PNNL.

Pacific Northwest is managed by DOE's Office of Science, but performs work for many DOE offices as well as other government agencies. Battelle has operated Pacific Northwest for DOE and its predecessors since 1965.

Pacific Northwest National Laboratory's core mission is to deliver environmental science and technology in the service of the nation and humanity. Through basic research PNNL creates fundamental knowledge of natural, engineered, and social systems that is the basis for both effective environmental technology and sound public policy. PNNL solves legacy environmental problems by delivering technologies that remedy existing environmental hazards, address today's environmental needs with technologies that prevent pollution and minimize waste, and are laying the technical foundation for tomorrow's inherently clean energy and industrial processes. PNNL also apply our capabilities to meet selected national security, energy, and human health needs; strengthen the U.S. economy; and support the education of future scientists and engineers.

The PNNL RA is subjected to review by local account and resource management authorities.

## *H.2 PNNL RA staff*

### H.2.1 Membership

Pacific Northwest National Laboratory's Registration Authority staff will serve as the Registration Authority staff for the Laboratory in support of Pacific Northwest's participation in the DOE GRIDS. These persons have been designated by PNNL and are PNNL staff members.

The initial set of persons to be included in the PNNL RA staff are responsible for implementing and ensuring the PNNL RA complies with both DOE GRIDS CA guidelines and existing PNNL authentication and authorization mechanisms. Additional persons may be appointed to the DOE GRIDS RA staff by PNNL.

### H.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the PNNL about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for PNNL. The POC shall be a member of the DOE GRIDS CA PMA.

## *H.3 PNNL Community*

The PNNL RA will serve the staff and affiliates of Pacific Northwest National Laboratory.

- Staff is defined as employees of the Laboratory.
- Affiliates are those individuals that are affirmed as collaborators by Pacific Northwest staff.

## *H.4 Authentication procedures*

### H.4.1 Authentication of individual identity

Pacific Northwest National Laboratory staff member will be identified by inspection of their badge. Inspection may take place in person by RA staff members or be conducted by a third party intermediary known and trusted by the RA staff. Trust is based on prior operational interaction with the RA staff.

Affiliates will be identified based on an affirmation by an PNNL staff member. The staff member will identified as detailed above.

### H.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between PNNL RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information. The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- Face-to-face conversation
- Telephone conversation between members of PNNL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed email between individuals with certificates from DOE GRIDS CA
- Paper documents physically signed and dated by either PNNL RA staff or DOE GRIDS CA staff

### H.4.3 Steps in authentication for certification

1. Individual requests a certificate from DOE GRIDS CA. In the case of an affiliate the request includes the name of PNNL staff member who will claim the subscriber as a collaborator. (secure means)
2. DOE GRIDS CA notifies PNNL RA of a certification request including the name, institution and email of the requester. (insecure means)
3. PNNL RA retrieves information of certification request from DOE GRIDS CA (secure means).
4. PNNL RA staff contact the requestor and verifies the requestor's identity.
5. If the subscriber is successfully vetted, PNNL RA staff approves certificate request (secure means).

## *H.5 Lifetime of certificates*

Certificates will be valid for one and half years and expire September 30$^{th}$ of each year.

## Appendix I: iVDGL RA operational procedures

The iVDGL RA will stop issuing new certificates as of Sept. 1, 2006. All continuing obligations of the iVDGL RA, including records retention and certificate revocation, are assumed by the OSG RA.

# I.1 Purpose, Goals, Scope

One of the Registration Authorities (RA) operating with some delegated authority of the DOE GRIDS CA is the international Virtual Data Grid Laboratory (iVDGL) Registration Authority (iVDGL RA). Information defining iVDGL is available at http://www.ivdgl.org/. This appendix describes how the responsibilities for the iVDGL RA are implemented. iVDGL is a creation of an NSF proposal to "provide a global computing resource for several leading international experiments in physics and astronomy, including the Laser Interferometer Gravitational-wave Observatory (LIGO), the ATLAS and CMS experiments at CERN, the Sloan Digital Sky Survey (SDSS), and the proposed National Virtual Observatory (NVO)." Use of the iVDGL has been and will continue to be extended to other projects, applications and experiment groups, through use of the Site Charter. The iVDGL project will exist for at least the 5-year funding period of that proposal, and if successful may become a more lasting entity. The need for the iVDGL RA itself will last as long as the laboratory does, and will at least cover the period where any X.509 certificates approved by this RA are still valid.

# I.2 iVDGL RA staff (sponsors)

## *I.2.1 Membership*

A number of persons are identified as comprising the iVDGL RA staff, which is the group of sponsors who are authorized to perform the identity check on individuals requesting a certificate. This list of persons is available to iVDGL members at (http://igoc.ivdgl.indiana.edu/RAinfo/rastaff.html). Each of these persons has a valid certificate from the DOE GRIDS CA. The initial set of persons to be included in the iVDGL RA staff is comprised of the PIs from each of the institutions funded by the iVDGL project and who have valid DOE GRIDS certificates.

Additional persons may be appointed to the iVDGL RA staff by the current members with the approval of the DOE GRIDS CA.

## *I.2.2 POC with DOE GRIDS CA*

All necessary communications between the DOE GRIDS CA and the iVDGL about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) which is a member of the iVDGL Operations Group. The POC shall be a member of the DOE GRIDS CA PMA.

# I.3 iVDGL VO Community

The iVDGL Virtual Organization community is defined as all persons authorized to use any of the iVDGL's on-line resources. Any one of the laboratory PI's may authorize a new member of the community. The privilege of requesting a certificate is subject to restrictions defined in this document.

# I.4 Authentication Procedure

## *I.4.1 Authentication of individual identity*

Any member of the iVDGL RA staff (a sponsor) may authenticate a person to satisfy a request from the POC. Person requesting certification must demonstrate reasonable evidence of membership in the iVDGL.

## *I.4.2 Communications*

All communications essential for authenticating individual identities and transmitting this information between iVDGL RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.

The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- Face-to-face conversation
- Telephone conversation between members of iVDGL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversations
- Secure digitally signed email between individuals with certificates from DOE GRIDS CA.

## *I.4.3 Steps in authentication for personal certification*

1. A person requests a certificate from DOE GRIDS CA; the request includes the name of an iVDGL RA staff member that can authenticate the request. (Secure means)
2. DOE GRIDS CA notifies iVDGL RA agents of a certification request. (Insecure means)
3. Agent notifies iVDGL RA staff member (sponsor) indicated in request that a request is pending including the name, institution and email of the requester (insecure means)
4. iVDGL RA staff (sponsor) contacts requester and authenticates request (secure means).
5. iVDGL RA staff notifies agent that authentication has occurred (secure means)
6. Agent notifies DOE GRIDS CA of the authentication of the request (secure means)

## *I.4.4 Steps in authentication for host/service certification*

1. At least one GridAdmin will be created by the iVDGL RA to handle host and service certificates per VO. A person send a request to the Grid Admin with the information from the grid-cert-request procedure. (Secure means)
2. The GridAdmin connects with the DOEGrids CA GridAdmin user interface and performs the necessary actions to have the certificated issues. This is documented in the GridAdmin User Guide (http://www.doegrids.org/Library/gridAdmin/gridAdminUser.html)

# I.5 Lifetime of certificates

Identity certificates approved by the iVDGL RA have a lifetime of no more than 12 months from date of approval.

# Appendix J: ESG RA operational procedures

## *J.1 Background*

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOE GRIDS CA is the Earth System Grid Registration Authority (ESG RA). Information defining the Earth System Grid VO is available at http://www.earthsystemgrid.org/. This appendix describes how the responsibilities for a VO RA are implemented for the ESG RA. The Earth System Grid II (ESG) is a new research project sponsored by the U.S. DOE Office of Science under the auspices of the Scientific Discovery through Advanced Computing program (SciDAC). The primary goal of ESG is to address the formidable challenges associated with enabling analysis of and knowledge development from global Earth System models. Through a combination of Grid technologies and emerging community technology, distributed federations of supercomputers and large-scale data & analysis servers will provide a seamless and powerful environment that enables the next generation of climate research.

It is expected that the ESG RA will have a finite lifetime and is implemented an example of a VO RA which can serve the needs of the ESG community until other persistent RA's are developed which serve this community.

## *J.2 ESG RA staff*

### J.2.1 Membership

A number of persons are identified as comprising the ESG RA staff. This list of persons is openly available on the ESG RA web site (e.g., http://www.earthsystemgrid.org/RA/). Each of these persons has a valid certificate from the DOE GRIDS CA.

The initial set of persons to be included in the ESG RA staff is representatives from ESG membership organizations. Additional persons may be appointed to the ESG RA staff by the ESG steering committee and approved by the DOE GRIDS CA.

### J.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the <VO> about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for the <VO>. The POC shall be a member of the DOE GRIDS CA PMA.

## *J.3 ESG VO Community*

The ESG Virtual Organization community is defined as all persons who are member of or collaborating with the software development working groups and Climate Experiments participating in ESG. These working groups and climate experiments are listed at http://www.earthsystemgrid.org/. The privilege of requesting a certificate is subject to restrictions defined in this document.

## *J.4 Authentication procedures*

### J.4.1 Authentication of individual identity

Any member of the ESG RA staff may authenticate a person to satisfy a request from the POC. Person requesting certification must demonstrate reasonable evidence of membership in the ESG VO.

### J.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between ESG RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.

The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

face-to-face conversation

telephone conversation between members of ESG RA staff

telephone conversation between individuals already personally known to each other from face-to-face conversations

secure digitally signed email between individuals with certificates from DOE GRIDS CA.

### J.4.3 Steps in authentication for certification

### J.4.3.1 Person Certificate

1. A person requests a certificate from the DOE GRIDS CA community Registration Manager (RM); the request includes the name of an ESG RA staff that can authenticate the request. (secure means)
2. DOE SG CA notifies ESG RA agents of a certification request. (insecure means)
3. Agent retrieves notification of certificate request from DOE GRIDS CA. (secure means)
4. Agent notifies ESG RA staff member indicated in the request that a request is pending including the name, institution and email of the requester. (insecure means)
5. ESG RA staff contacts requester and authenticate request. (secure means)
6. ESG RA staff notifies agent that authentication has occurred. (secure means)
7. Agent notifies DOE GRIDS CA of the authentication of the request using RM software. (secure means)
8. Person requesting certificate receives notification from RM.

### J.4.3.2 Host or Service Certificate

1. A person requests a host or service certificate from the DOE GRIDS CA community RM.
2. Agent receives notification of request and takes assignment if appropriate for this RA.
3. Agent checks if person has a valid DOE GRIDS CA certificate.

4. Agent approves request if person has a valid DOE GRIDS certificate and rejects request if person does not have a valid DOE GRIDS certificate.

## *J.5 Lifetime of certificates*

Identity certificates approved by the ESG RA have a lifetime of no more than 12 months from date of approval.

# Appendix K: FNAL RA operational procedures

## *K.1 Background*

The Fermi National Accelerator Laboratory's (FNAL) DOE GRIDS RA is intended to serve the staff and collaborators of the Laboratory. The Laboratory is described at http://www.fnal.gov/ and is a DOE laboratory focused on the advancement of High Energy Physics. This appendix describes how the responsibilities for FNAL RA are implemented at FNAL.

## *K.2 FNAL RA staff*

### K.2.1 Membership

Fermi National Accelerator Laboratory's Registration Authority staff will serve as the Registration Authority staff for the Laboratory in support Fermi's participation in the DOE GRIDS. These persons have been designated by FNAL and are FNAL staff members.

The initial set of persons to be included in the FNAL RA staff are responsible for implementing and ensuring the FNAL RA complies with both DOE GRIDS CA guidelines and existing FNAL authentication and authorization mechanisms. Additional persons may be appointed to the DOE GRIDS RA staff by FNAL.

### K.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and FNAL about policy and practices pertaining to the duties of the RAs, as defined in this document, are transmitted via the Point of Contact (POC) for FNAL. The POC shall be a member of the DOE GRIDS PMA.

## *K.3 FNAL Community*

The FNAL RA will serve the staff and affiliates of Fermi National Accelerator Laboratory.

- Staff is defined as employees of the Laboratory.
- Affiliates are those individuals that are affirmed as collaborators by Fermi staff.

## *K.4 Authentication procedures*

### K.4.1 Authentication of individual identity

Fermi National Accelerator Laboratory will be providing identity certificates to their staff and affiliates by operating its own KCA. There will be limited use of DOEGrids Identity certificates.

Fermi National Accelerator Laboratory's staff members and affiliates will be identified by inspection of their badge or strong authentication via FNAL's Kerberos realms. The FNAL strong authentication program is described at http://www.fnal.gov/docs/strongauth/ . Inspection of badges may take place in person by RA staff members or be conducted by a third party intermediary known and trusted by the RA staff.

### K.4.2 Communications

All communications essential for authenticating individual identities, their requests and transmitting this information between FNAL RA staff and the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information. The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- Face-to-face conversation
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed communications between individuals with certificates from DOE GRIDS CA or from the FNAL KCA.
- FNAL-realm Kerberos authenticated requests.
- Paper documents physically signed and dated by either FNAL RA staff or DOE GRIDS CA staff

### K.4.3 Steps in authentication for certification

### K.4.3.1 Interactive Method

1. Individual requests a client or service certificate from DOE GRIDS CA. In the case of an affiliate the request includes the name of FNAL staff member who will claim the subscriber as a collaborator. (secure means)
2. DOE GRIDS CA notifies FNAL RA of a certification request including the name, institution and email of the requester. (insecure means)
3. FNAL RA retrieves information of certification request from DOE GRIDS CA (secure means).
4. FNAL RA staff contact the requestor and verifies the requestor's identity or right to have a service certificate.
5. If the subscriber is successfully vetted, FNAL RA staff approves certificate request (secure means).

### K.4.3.2 Batch Method

1. Individual requests a client or service certificate from a FNAL RA agent. (secure means)
2. FNAL RA staff verifies the requestor's identity and right to have a service certificate.
3. If the request is successfully vetted, FNAL RA staff approves certificate request (secure means).

## *K.5 Lifetime of certificates*

Certificates will be valid for one year from date of issuance.

# Appendix L: Guidelines for Security Incident Response and Resolution

## *L.1 Background*

Compromise or loss of a private key is a serious issue that requires cooperation amongst all participating DOE Grids PKI members, subscribers and relying parties to minimize the extent of damage. These guidelines are meant only to provide guidance for the DOE Grids PKI members to resolve these incidents since every incident will be unique.

## *L.2 Definitions*

**Security Incident**

An incident that has the potential of private key loss or compromise, regardless if the compromise or loss was successful. Such incidents include but are not limited to user credential compromise, privilege escalation on systems known to contain private keys, accidental exposure of private keys to unauthorized third parties or loss of a private key.

**Incident Response Team**

Consist of members of the DOE Grids PKI PMA, which are responsible for evaluating security incidents and presenting their recommendations to the DOE Grids PKI members. This team shall consist of volunteers from within the DOE Grids PKI PMA and shall number no less than three. Members shall be appointed by the DOE Grids CA managers if insufficient volunteers are present.

## *L.3 Responsibilities*

1. **RA Points of Contact (POC)**
   a. The POC's will act as the coordinating liaison between the DOE Grids PKI and their VO's computer security for incident communication and resolution.
   b. Within 12 hours of initial discovery of a security incident, the POC shall notify the DOE Grids PKI members in a secure manner.
   c. The POC shall work with their RA computer security to determine the extent of the incident and the keys that have been potentially compromised. This information shall be relayed to the DOE Grids PKI members as soon as possible.
   d. The POC's are encouraged to share what information they have about a security incident with the DOE Grids PKI members, especially the incident response team.

2. **DOE Grids CA operations staff**
   a. The CA operations staff will communicate with the involved System Administrators and Relying parties to gather information on the certificates that are suspected of compromise.
   b. They will report to the DOEGrids PMA their findings.
   c. They will respond to the directions from the PMA or the Incident Response team.

3. **Incident Response Team**

a. The Incident Response Team will be formed by the DOE Grids PMA upon notification of a security incident.
b. The Incident Response Team shall evaluate all information regarding an incident.
c. A recommendation for course(s) of action will be presented to the DOE Grids PKI. These recommendations shall consist, to the greatest extent possible, an evaluation of risk associated with each course of action recommended.

## *L.4 Actions*

1. If evidence is presented that a private key has been compromised, the key shall be immediately revoked.

2. If insufficient information is presented to verify that a suspected key has been compromised, the DOE Grids PMA will convene to evaluate the recommendations put forth by the Incident Response Team. The DOE Grids PMA will vote on the recommendation(s) presented by the Incident Response team. This vote will be an advisory vote only.

3. The Incident Response Team will write a summary of the incident and the results of any advisory vote for the DOE Grids PMA. This summary will be available to all DOE Grids PKI members and will be archived for future reference if necessary.

# Appendix M: LCG RA operational procedures

## *M.1 Background*

The Large Hadron Collider (LHC) Computing Grid (LCG), www.cern.ch/lcg, is a large grid deployment project supporting particle physics experimental collaborations using the LHC particle accelerator at CERN. These collaborations, or Virtual Organizations (VO), are worldwide in scope, highly distributed and involve thousands of scientists at hundreds of institutions. Whilst the majority of the authentication requirements for the LCG VOs are met by a set of trusted national Certification Authorities, the need to reliably generate authentication credentials for individuals and resources not covered by one of these approved CAs still exists. This need for a "catch-all" is met by the LCG RA.
Almost by definition, individuals requesting certificates from the LCG RA are geographically widely dispersed. Because of this, face-to-face meetings for exchange of authentication information and personal knowledge authentication criteria are not always applicable. By specifying a set of authentication requirements and procedures this appendix describes how the responsibilities for a VO RA are implemented by the LCG RA.

## *M.2 LCG RA staff*

### M.2.1 Membership

The RA consists of at least two named individuals appointed by the LCG Security Group and approved by DOE GRIDS CA. Each of these persons will have a valid DOE GRIDS CA certificate. RAs may appoint Registration Agents (RAgs) at Participating Institutes (see 1.3 below). RAgs will have a valid DOE GRIDS CA certificate and be classed as RA staff. A RAg will be appointed where total membership or affiliation at their institute is expected to require a number of DOE GRIDS CA certificates to be issued. It is expected that a RAg will hold a long term appointment with their institute.

### M.2.2 Point of Contact (POC) with DOE GRIDS CA

The LCG Security Group shall identify an individual to be the Point of Contact with DOE GRIDS CA. All necessary communications between the DOE GRIDS CA and the LCG RA about policy and practices pertaining to the duties of the RAs and RAgs as defined in this document are transmitted via the Point of Contact (POC) for the LCG RA (www.cern.ch/lcg/catch-all-ca). The POC shall be a member of the DOE GRIDS CA PMA.

## *M.3 LCG RA VO Community*

The LCG RA VO Community members are defined as EITHER:

- any person who is officially part of a recognized LCG VO and who is not covered under the policy of an existing approved LCG CA
- any person who requires such a certificate exclusively for the purposes of software testing, deployment or other activity related to LCG.

Members of the LCG RA VO Community must be attached to a Participating Institute.
A Participating Institute is defined as EITHER of:

- An institute for which a RAg has been appointed and for which there is a written agreement between the RA and the RAg that the RAg may authenticate individual identity.
- An institute for which the RA is able to obtain reasonable assurance (e.g. from VO or LCG project management) that its members or affiliates are participating in LCG.

## *M.4 Authentication procedures*

### M.4.1 Authentication of individual identity

In all cases the RA staff must possess reasonable assurance of participation by the subscriber in the LCG RA VO Community as defined in section 1.3 above.
Individuals will be authenticated if they show possession of BOTH the following documents which MUST state the full name of the individual applying for the certificate:

- A document proving current affiliation to a Participating Institute.
- A valid official or government photo identity such as passport or driving license.

RA staff may at their discretion request additional supporting evidence of identity.
Each RAg will only authenticate identity for an agreed set of Participating Institutes as defined in 1.3.

#### M.4.1.1 Authentication without face-to-face meeting

Authentication without a face-to-face meeting will only be used between the subscriber and the LCG RA. RAgs WILL NOT authenticate without face-to-face meeting.
For the purposes of exchange of authentication documents, the postal or facsimile transmission of high quality copies will be acceptable where supplemented by a telephone conversation, instigated by the authenticating party, using a publicly available telephone number or other of the means of secure communications listed below. In this case the date and time of transmission should be confirmed.

### M.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between LCG RA staff and the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.
The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.
The means of secure communications acceptable are:

- face-to-face conversation
- telephone conversation between members of LCG RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- secure digitally signed email between individuals with certificates from an approved CA

### M.4.3 Steps in authentication for certification

The steps in authentication for certification take two paths depending on whether a supporting RAg is already appointed. The procedure for authentication for a RAg is the same as for a person without a RAg. It is expected that a RAg will always be appointed where there is a need for host or service certificates.

#### M.4.3.1 Personal Certificate

##### M.4.3.1.1 Personal Certificate without RAg

1) A person requests a certificate from the DOE GRIDS CA community RM.
2) The LCG RA receives the notification of request and, if appropriate for this RA, takes assignment.
3) The LCG RA authenticates the identity of the individual as defined in section 1.4.1.
4) The LCG RA approves or rejects the request using the community RM.

5) The person requesting the certificate receives notification from RM.

#### M.4.3.1.2 Personal Certificate with RAg

1) A person requests a certificate from the DOE GRIDS CA community RM.
2) The LCG RA receives the notification of request and, if appropriate for this RA, assigns it to an appropriate LCG RAg.
3) The LCG RAg authenticates the identity of the individual as defined in section 4.1.
4) The LCG RAg approves or rejects the request using the community RM.
5) The person requesting the certificate receives notification from the RM.

### M.4.3.2 Host Certificate

1) A person requests a host or service certificate from the DOE GRIDS CA community RM.
2) LCG RA receives notification of the request and assigns it to appropriate LCG RAg if appropriate for this RA.
3) LCG RAg checks if the person has a valid DOE GRIDS CA certificate.
4) LCG RAg checks if the requested host or service CN specifies a FQDN located within the domain of the Participating Institute.
5) LCG RAg approves the request if all the conditions listed above are met and rejects the request otherwise.

## M.5 Lifetime of certificates

Identity certificates approved by the LCG RA have a lifetime of no more than 12 months from date of approval.

# Appendix N: Open Science Grid (OSG) RA operational procedures

## *N.1 Background*

One of the Registration Authorities (RA) operating with some delegated authority of the DOE GRIDS CA is the Open Science Grid Registration Authority (OSG RA). Information defining the OSG VO is available at http://www.opensciencegrid.org/. This appendix describes how the responsibilities are implemented for the OSGG RA.

The OSG has an operational model (http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=47) where "Support Centers" are identified to handle support issues for users, VOs, resources, etc. and the communication of these issues with OSG Operations and the Grid Operations Center (GOC). In general, functions of the OSG RA are to be handled as part of the Support Center functions where each Support Center has a defined scope of VOs and resource domains for which they are responsible. Any requests that are not claimed one of the Support Center's agents in a reasonable time will be handled by the GOC, or by the POC.

OSG has assumed all continued obligations for the PPDG and iVDGL RAs.

## *N.2 OSG RA staff*

### N.2.1 Membership

A number of persons are identified as comprising the OSG RA staff. These persons are authorized as agents for the purpose of processing certificate enrollment and revocation requests. In general, Registration Authority Agents are part of a Support Center participating in OSG. A list of OSG Support Centers is given at http://www.opensciencegrid.org/index.php?option=com_content&task=view&id=37&elMenu=Grid%20Support. The means of contacting the OSG RA staff is published at the RA web site (www.opensciencegrid.org/ra).

### N.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the OSG about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for OSG. The POC shall be a member of the DOE GRIDS CA PMA.
Currently the POC is

Doug Olson, LBNL
dlolson@lbl.gov
(510) 486-4567

Communication with the OSG RA on operational issues should be via the email address osg-ra@opensciencegrid.org. This address will forward mail to the POC named above, as well as to the OSG Grid Operations Center.

## *N.3 OSG Community*

The Open Science Grid community is defined as all persons who are members of or collaborating with the Virtual Organizations registered with OSG as well as all resource and service providers (see http://osg-vors.grid.iu.edu/) and members of the OSG Consortium.

On a case-by-case basis the OSG RA will consider processing requests from people who are not participating in OSG but otherwise qualify for a DOEGrids certificate (i.e., satisfy

the ESnet AUP) and are not covered by any of the existing DOEGrids RAs. These cases will be handled only on a "best effort" basis and there is no guarantee of performance beyond maintaining the quality of the authentication.

## *N.4 Authentication procedures*

### N.4.1 Authentication of individual identity

Any member of the OSG RA staff may authenticate a person to satisfy a request from the CA.

An RA staff person may accept attestation for the subscribers identity from an authoritative source such as a supervisor with line management authority at the subscribers institution of employment (or enrollment for students), or equivalent authoritative persons of the VO of which the subscriber is a member. Such an authoritative person for this certificate request is called a Sponsor. Each Support Center will decide which individuals are qualified to be Sponsors within their domain of support. In this case the RA staff must authenticate the Sponsor's identity and his/her relation to the Subscriber in order to accept the confirmation of the Subscriber from the Sponsor. The actual Sponsor used to authenticate the request may or may not be the same Sponsor as listed by the Subscriber in the request.

For cases where a Sponsoring individual has not or can not be authenticated as stated above, an RA staff person may authenticate the subscriber directly with additional corroborating information about the subscriber which is obtained out of band relative to the certificate request. Such corroborating information includes, but is not limited to,

1. Name, email address and telephone number available from a publicly accessible directory of the institution where the subscriber is affiliated.
2. Unsigned email from third parties known to the RA staff person attesting to the validity of the request
3. 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.
4. Information about the subscriber in other established public forums, such as conference web sites or public discussion groups.
5. Personal telephone call with the subscriber by the RA staff where subscriber describes the purpose and intended use of the certificate

Suitable authentication will include several pieces of corroborating information and the information used for the authentication will be recorded as part of the authentication record in place of the Sponsor confirmation. All requests authenticated by this method require notification of the RA.

### N.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between OSG RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information.

The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- face-to-face conversation
- telephone conversation between members of OSG RA staff
- telephone conversation between individuals already personally known to each other from previous experience
- secure digitally signed email between individuals with certificates from DOE GRIDS CA.

## N.4.3 Steps in authentication for certification

### N.4.3.1 Person Certificate

1. A person requests a certificate from the DOE GRIDS CA.
2. Agent receives notification of request and takes assignment if appropriate for this RA.
3. Agent contacts and authenticates a Sponsor if necessary for this request.
4. Sponsor confirms or refutes request to Agent, if a Sponsor was involved.
5. Agent approves or rejects request using RM.
6. Agent logs summary of actions (see section N.4.4)
7. Person requesting certificate receives notification from RM.

### N.4.3.2 Service Certificate

In case of a requestor not using the GridAdmin interface and authorization:

1. A person requests a host or service certificate from the DOE GRIDS CA.
2. Agent receives notification of request and takes assignment if appropriate for this RA.
3. Agent checks if person has a valid DOE GRIDS CA certificate, or authenticates request as for a Person Certificate (N.4.3.1).
4. Agent checks if the DN is new and unique and, if so, continues to process request. If DN already exists agent verifies that requester is registered owner of the DN and, if so, continues to process the request. If requestor is not the registered owner of the DN the agent either handles a transfer of ownership for the DN or rejects the request. In case of transfer of ownership, all previous certificates with the same DN will be revoked.
5. Agent approves request if subscriber is successfully authenticated (step 3) and has been registered as the owner of the DN (step 4).
6. Agent logs summary of actions (see section N.4.4).

A subscriber using the GridAdmin interface uses the procedures for GridAdmin requests as described in Appendix A.

## N.4.4 Logging

For each request processed by an agent (certification or revocation) a summary message of this action will be sent via email to osg-ra-log@opensciencegrid.org. An agent of the OSG RA working within a VO support organization an record action summary messages to an archive maintained within the VO support organization instead of the osg-ra-log@opensciencegrid.org. In this case, the agent is responsible that the message archive is maintained and accessible to the OSG RA. This summary message should contain the following information:

- Request identifier (for certification requests)
- Description of action take (approve, reject, cancel, revoke, …)
- Name and/or individual email address of Agent who processed the request.

- Name of Sponsor who confirmed the request (in some cases the Agent is also the Sponsor).
- For certification requests, statement of why the requestor qualifies to receive certificate, i.e., membership in a particular VO, or association with a science program participating with OSG.
- Certificate serial number (if applicable)
- Certificate subject name, i.e., DN (if applicable)

## *N.5 Revocation procedures*

The revocation procedure is initiated immediately upon receipt of a revocation request by any member of the OSG RA staff. Revocation requests must be authenticated as described elsewhere in this document.

The following steps describe the revocation procedure to be used for any certificates issued by the OSG RA.

1. Receive revocation request
   The time that the revocation request is first sent to the OSG RA defines a timestamp which is used to start a time limit clock for processing the request, call it the "revocation clock".
2. Notify DOEGrids CA managers and the OSG RA POC of receipt of revocation request.
3. Authenticate revocation request.
4. Write description of circumstances leading to revocation request and send to OSG RA POC. Include in this description whether or not the certificate in question has been revoked yet.
5. The POC, at his/her discretion, may investigate the occurrence and decide if revocation is warranted.
6. Within a one business day time limit for the revocation clock, the agent handling the revocation request will notify the DOEGrids CA managers of the disposition of the request, whether or not the certificate has been revoked. If the certificate has not been revoked then a clear description of why revocation was not necessary must be included in the notice.
7. Upon reaching the one business day time limit on the revocation clock the DOEGrids CA managers can take further action on the revocation request, including revoking the certificate if they determine it is necessary even if the OSG RA objects.

If any member of the OSG RA staff receives a revocation request for a certificate NOT issued by the OSG RA then the following action will be taken.

1. Forward the revocation request to the DOEGrids CA managers and the issuing RA (if possible) upon receipt of such request, and forward a copy of the notice to the OSG RA POC.
2. The OSG RA POC, at his/her discretion, will decide if any additional action is necessary by the OSG RA.

## *N.6 Lifetime of certificates*

Identity certificates approved by the OSG RA have a lifetime of no more than 12 months from date of approval.

## *N.7 Cyber Protection Plan*

The Open Science Grid Registration Authority functions as part of the OSG Facility Operations and the cybersecurity plan is part of the overall OSG cybersecurity plan. As of the writing of this CPS appendix the OSG CyberSecurity Protection Plan is being developed. The plan will identify the assets of OSG used for the RA functions, a risk

analysis, controls, maintenance and evaluation procedures, and the relation between the OSG RA, the DOEGrids CA and the VOs that also carry out part of the RA function.

# Appendix O: General Guidelines for DOEGrids CA operations

## O.1 Background

The DOEGrids Certificate Authority is run and operated by ESnet for the DOEGrids PMA. This includes all the hosts and security systems required to run the service. The team that will be providing this service will be known in this document as the "DOEGrids Operations staff". This is not a Grid Virtual Organization. Certificates are issued to CA operations and some RA/Agents for the purpose of issuing certificates to the DOEGrids community.

DOEGrids operations staff will only use security tokens for protecting the private key of each staff member. These are the keys that are used to manage the DOEGrids Certificate Authority.

This appendix will focus on the general operations of the Public Key infrastructure used by DOEGrids. In § 2.1 general obligations for the Certificate Authority and Registration Authorities were defined. In Appendix A of this document additional guidance for Registration Authorities is presented. This Appendix will be used for additional guidance for the CA operations.
This appendix has two primary sections. In CA operations Staff, each role used to manage the DOEGrids PKI is defined. In section CA operations, tasks and responsibilities are enumerated.

## O.2 CA operations staff

The DOEGrids operations staff has defined a number of roles to be used to manage the PKI used by DOEGrids. The operational staff of the DOEGrids CA service consists of:

1. CA managers
    a. CA admin
    b. HSM admin
    c. HSM operator
    d. Registration Authority
2. Host admin
3. Data Center Security
    a. Vault operator
    b. Rack operator
    c. Rack Admin
4. Firewall admin
5. IDS manager

## O.3 CA operations

The DOEGrids operational staff have the following duties and responsibilities.

1. Responsible for configuration, starting and stopping of service.
2. Need to issue Certificates to CA staff members for primary use with the DOEGrids CA.
3. Need to issue Host certificates for CA operations.
4. Responsible for the DOEGrids RA and Agents certification process
    a. For initial boot strapping the process. RA is responsible for future renewals.
    b. The procedures and process are the responsibility of the DOEGrids PMA. It is the responsibility of the DOEGrids operations staff to execute these policies.

5. Revocations that are not handled by the responsible RA will be done by the CA operations staff.
    a. CA operational staff has the authority to revoke any certificate issued by DOEGrids.
    b. Routine Revocation must be validated by a signed email from requestor. We will determine if the request is valid or appropriate.
    c. Emergency: CA operations staff will revoke certificates as required by the DOEGrids Security response committee or as they deem necessary and appropriate.
    d. We will report all emergency revocations to the DOEGrids PMA.
6. All bounced email notices for certificate renewals will be referred to the responsible RA.
7. CA operations may revoke certificates when the registered email bounces.
8. CA operations may revoke Host certificates after the expiration dates.

# Appendix P: Philips Research (US) RA operational procedures

## *P.1 Background*

Philips Research (Briarcliff) is an organizational division of Royal Philips Electronics involved in basic and applied research. It is involved in non-competitive and pre-competitive collaborative research in the context of the LHC Computing Grid, the Enabling Grid for e-Science e-infrastructure and national Grid infrastructures, and has several collaborative programs with US government agencies and organisations, such as but not limited to DARPA (e.g. in the DBAC – Deep Bleeding Acoustical Coagulation project) and NIH.

This appendix describes how the responsibilities for a VO RA are implemented for the Philips Research (US) RA.

The need for the Philips Research (US) RA is permanent for the foreseeable future and will be the primary authentication and authorization mechanism for researchers in the US and grid-accessible computer systems in the US to connect to and use the grid.

## *P.2 Philips Research (US) RA staff*

### P.2.1 Membership

A number of persons are identified as comprising the Philips Research (US) RA staff. These persons have been designated by Philips Research and are Philips Research staff members. Each of these persons has a valid certificate from an IGTF Accredited Classic CA.

The initial set of persons to be included in the Philips Research (US) RA staff are responsible for implementing and ensuring the Philips Research (US) RA complies with both DOE GRIDS CA guidelines and also pre-existing Philips Research authentication and authorization mechanisms.

### P.2.2 Point of Contact (POC) with DOE GRIDS CA

All necessary communications between the DOE GRIDS CA and the Philips Research (US) VO about policy and practices pertaining to the duties of the RAs as defined in this document are transmitted via the Point of Contact (POC) for the Philips Research (US) VO. The POC shall be a member of the DOE GRIDS CA PMA.

Communication with the Philips RA on operational issues should be via the email address al_doegrid_poc@natlab.research.philips.com. This address will forward mail to the Philips Research (US) POC. Alternate email address: ronald.van.driel@philips.com.

## *P.3 Philips Research (US) Community*

The Philips Research (US) community is defined as all persons who are authorized to utilize Philips Research (US) resources and computer systems owned and operated by Philips

Research and located in the US. The privilege of requesting a certificate is subject to restrictions defined in this document.

## *P.4 Authentication procedures*

### P.4.1 Authentication of individual identity

Authentication of an individual identity must follow existing Philips Research (US) guidelines for client authentication. Persons requesting certification must demonstrate reasonable evidence of membership in the Philips Research (US) community. All individuals must avail over computer accounts and valid staff registration using the methods used to authenticate all personnel and guests at the laboratories and facilities of Philips Research US. using the methods used to authenticate all personnel and guests at the US laboratories and facilities of Philips Research. The account support staff will contact the Philips Research (US) RA POC regarding the results of the authentication procedure.

### P.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between Philips Research (US) RA staff to the DOE GRIDS CA are carried out in a secure manner. In this context, secure means the information is not changed by third parties but does not mean that third parties may not observe the information. The secure communications may be supplemented by insecure communications as long as the essential information is verified by a secure means. For example, information about a certification or revocation request may be transmitted by insecure email as long as it is verified by secure means before transmission to the DOE GRIDS CA.

The means of secure communications acceptable are:

- Face to face conversation.
- Videoconference (telephone) conversation between members of Philips Research (US) RA staff.
- Videoconference (telephone) conversation between members of Philips Research (US) RA staff and Philips Research users at telephone number listed in institutional phone book. User is authenticated by Philips Research (US) RA staff based on information stored in the corporate directory of Royal Philips Electronics.
- Secure digitally signed email between individuals with certificates from an IGTF Accredited classic CA.
- Paper documents physically signed and dated by either Philips Research (US) RA staff or DOE GRIDS CA staff

Note that face to face communication may not always be feasible, because Philips Research (US) includes geographically distributed users. In this case, user verification is based on information obtained from out of band communication during the initial Philips identity verification and ID process.

All instances of communication essential for authenticating individual entities will be logged and archived by Philips Research (US) RA staff. This archive will only be accessible to Philips Research (US) RA staff and other authorized agents and will contain the date and time of the communication, names of the parties involved in the communication, name of individual the communication is in regards to and any other pertinent information that would be deemed essential to reconstruct the communication if so required.

### P.4.3 Steps in authentication for certification

1. Individual requests a certificate from DOE GRIDS CA, the request includes the name of Philips Research (US) VO who will authenticate the request. (secure means)
2. DOE GRIDS CA notifies Philips Research (US) POC and Philips Research (US) RA staff of a certification request. (insecure means)
3. Philips Research (US) RA Staff retrieves information of certification request from DOE GRIDS CA (secure means).
4. Philips Research (US) RA staff member looks up requestor contact information in the *Management database*. This will be used for establishing a secure means to authenticate the user. Requestor MUST be an existing *Philips Research affiliate, with an existing account*.
5. Philips Research (US) RA staff member contacts requestor via secure channel and authenticates individual per existing Philips Research (US) authentication policy and mechanisms. (secure means)
6. Philips Research (US) RA staff member logs the communication used to authenticate the requestor, as described in this document.
7. Philips Research (US) RA staff member notifies Philips Research (US) POC that authentication has occurred (insecure means)
8. POC calls Philips Research (US) RA staff at telephone number listed in institutional phone book, and verifies status of authentication (secure means)
9. POC or Philips Research (US) RA Staff notifies DOE GRIDS CA of the authentication of the request (secure means)

The above procedure only applies to authentication for existing members of the Philips Research (US) community. The Philips Research (US) RA will not issue certificates to a requester *that does not have an existing Philips Research identity*. Initial user verification during the allocation process is described in P.4.2.

## *P.5 Lifetime of certificates*

Identity certificates approved by the Philips Research (US) RA have a lifetime of no more than 12 months from date of approval.

## Bibliography

[Bro] V. Paxson, Bro: A System for Detecting Network Intruders in Real Time, Computer Networks, 31(23-24), pp. 2435-2463, 14 Dec. 1999. (This paper is a revision of paper that previously appeared in Proc. 7th USENIX Security Symposium , January 1998.) http://www.icir.org/vern/papers.html

[INFN CP] http://security.fi.infn.it/CA/CPS/ INFN CA Policy and CPS.

[GridCP] http://gridcp.es.net/ Global Grid Forum CP

[EuroPKI] - EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000

[FBCA] - X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999

[NCSA] - National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999

[OpenSSL] - http://www.openssl.org/

[PAG] American Bar Associations PKI Assessment Guidelines ("PAG") http://www.abanet.org/scitech/ec/isc/pag/pag.html

[Proxy] – Tueche, S., et al., Internet X.509 Public Key Infrastructure Proxy Certificate Profile. 2001, IETF draft.

[RFC2459] - R. Housley, W. Ford, W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999

[RFC2527] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999

[TrustID] - TrustID Certificate Policy http://www.digsigtrust.com/certificates/policy/tsindex.html

## List of Changes

| VERSION | DATE | CHANGES |
|---|---|---|
| **1.0** | **Nov 16, 2001** | **Initial Release based on INFN CP/CPS** |
| **1.1** | **Nov 30, 2001** | **Section 1.1: Added text to assign DOE GRIDS PMA responsibility for CP/CPS maintenance<br>Section 2.1: Split CA and RA obligations<br>Section 3.1.1/7.1.4: Changed host name requirement - Von Welch's text added<br>Section 4.2: Added certificate life cycle text<br>Section 4.4: Did a little more on Revocation process/reasons.** |
| **2.0** | **May 15, 2002** | **Added RA support, including Appendixes for PPDG, FNC and RA guidelines. Redid format and reviewed/rewrote all sections of the CP-CPS<br>Numerous modifications to text based on input from PMA** |
| **2.1** | **Aug 26, 2002** | **Add iVDGL and ESG appendixes** |
| **2.2** | **Oct 15, 2002** | **The following list the changes for this version:<br>1. Authentication of organization identity - document our current practice Check PAG section D.3.2.5 for additional information.<br>o Moved and described in the new PMA charter document<br>2. Sec 1.1 add ESnet's relationship to LBNL<br>o Added<br>3. sec 1.3.1 add system architecture delineate what parts are managed by ESnet and other organizations.<br>o Added, including table of components.<br>4. sec 2.1.2 add subscriber definition<br>o Added to general definitions sec 1.1.1<br>5. Add Acronym definitions<br>o What Acronyms?<br>6. sec 3.1.5 clean up the definition of how we do Individual identity. Also how RM's will be used and deployed - tie to sec 1.3.1.<br>o Added text and link to certificate work flow<br>7. sec 4.2.2 Format error and redundant information<br>o could not find - old problem??<br>8. App A A.2, item 8 Add emphasize that the Rags may NOT do the following...** |

| | | |
|---|---|---|
| | | ○ **Changed.**<br>9. **Replace section 6.1.9 with input from list.**<br>○ **Replaced with Von's input**<br>10. **CRL distribution point located in PKI1 certificate. Where should it point to?**<br>○ **Changed 2.1.4 to reflect the new repositories.**<br>11. **How to vet new RAs?**<br>○ **Moved and described in the new PMA charter.**<br>**Other changes:**<br>1. **Changed the title of the doc to reflect new Name - DOE Grids**<br>2. **Global change of DOESG for DOE Grids**<br>3. **Changed 1.2 to reflect new name version...**<br>4. **Changed link to point to new site.**<br>5. **changed 1.3.2**<br>6. **changed 2.1.1 certificate life time to 12 months. EDG requirement??**<br>7. **Changed 6.3 CA certificate life time to 5 years. EDG requirement??**<br>8. **7.1.4 changed names to doegrids.** |
| **2.3** | **Dec 15, 2003** | 1. **7.1.4 Add dotted IP for hosts in service section**<br>2. **Change the DOE science grid links to DOEGrids.org links - section 2.1.3**<br>3. **6.2.3 and 6.4 describe the use of FIPS 140 device…**<br>4. **2.6.4 change "repository" location**<br>5. **8.2 change policy publication point**<br>6. **3.1.3 typo hared - > Shared**<br>7. **3.1.4 Changed from no stipulation to document current practices.**<br>8. **3.1.5 Changed Local polices to RA polices.**<br>9. **7.1.4 Changed example of IP octet value to a unique one.**<br>10. **Editorial change this table to have visible dividers.** |
| **2.4** | **May 31, 2004** | 1. **Add in the FNAL appendix (K)**<br>2. **Add in Steve Lau appendix (L)**<br>3. **Editorial changes by Doug Olson**<br>4. **Added more contact information**<br>5. **Added more to the CA ,RA , subscribers and Relying party responsibilities to deal with security incidents.**<br>6. **Add LCG Catch-all RA appendix (M)** |
| **2.5** | **August 12, 2004** | **Added NCC- EPA appendix (N)** |
| **2.6** | **December 15, 2005** | **Changes Made:**<br>**Doug:**<br>1. **Mod Glossary Added Owner, registered owner to glossary, modified Subscriber** |

| | | |
|---|---|---|
| | | **definition.**<br>**2. Mod text in section 1.3.3 (end entity)**<br>**3. Mod text 2.1.1 adding DN to registered owner requirements.**<br>**4. Mod text 2.1.2 adding the user must verify the DN does not exist or that they are the owner.**<br>**5. Mod 3.1.3 added User can have multiple Certs with same name.**<br>**6. Mod 4.1 added text to allow script access to website.**<br>**7. Mod 4.2 so RA must verify EE is owner of requested DN.**<br>**8. Mod 4.4.1 Revoke old certs when DN is transferred to new owner.**<br>**9. Mod 7.1.4 Name forms clean up**<br>**10. Add a sentence in 2.1.1 for the RA obligations: Verify that the entity…**<br><br>**Mary:**<br>**1. Mod Glossary end entity definition.**<br>**2. Mod 7.1.4 Name forms clean up**<br><br>**Tony:**<br>**1. Clean up text in sec 1.3.1**<br>**2. Mod 2.1.4 corrected URLs**<br>**3. Mod 2.6.4 added third party pup points.**<br>**4. Mod 4.4.6 changed OCSP to experimental only service.**<br>**5. Mod 1.2 and 7.1.6 changed OIDs**<br>**6. Mod 7.1.4 Name forms clean up.**<br>**7. Mod Appendix A major rewrite.**<br>**8. Mod Appendix A added RA and Agent letters.**<br>**9. Mod Appendix A added DN ownership verification as a RA or Agent responsibility.**<br>**10. Replaced iVDGL appendix with their new content.**<br>**11. Mod Appendix L added CA operations requirements.**<br>**12. Mod Appendix A: RA letters, Grid Admin, etc.**<br>**13. Changed to using V2 CRLs**<br>**14. Removed EPA**<br>**Mike:**<br>**1. Removed the Root CA details.**<br>**2. Modified AUP text**<br>**3. Modified Trouble reporting text.**<br>**4. Modified LDAP access text.**<br>**5. Moved HSM description to 6.8.**<br>**6. Modified Certificate Extensions text.**<br>**7. Removed wrong Grid Admin text.** |
| **2.7** | **July 1, 2006** | **The following changes were done by Doug** |

| | | |
|---|---|---|
| | | **Olson, Mary Thompson and Tony J. Genovese**<br>**1. §1.1 added warning not to base Authorization on DOEGrids ID certs.**<br>**2. § 1.2 added new OID for this version.**<br>**3. § 2.1 added general obligations for all RAs, Agents and Subscribers.**<br>**4. §2.1.1 added that RAs will be notified about Revocation requests. Changed entity to person. Added must maintain record of authentication process and revocation requests.**<br>**5. §2.4.1 added LBNL to the list of laws we fall under.**<br>**6. §4.1 modified text to reflect current work flow**<br>**7. §4.2 new section on Certificate Request cancellation**<br>**8. §4.5.3 Modified Revocation request process.**<br>**9. §4.7.1 added revocation requests to the events recorded list.**<br>**10. §7.1.2 modified RFC822Name to allow individual or Group names**<br>**11. Added appendix N for OSG.** |
| **2.8** | **21 August 2006** | **1. Replace ORNL appendix with updated version.**<br>**2. Added to A.1 information describing the role of DOEGrids operations WRT vetting RA/Agents**<br>**3. Modified 2.1, 4.5 and added Appendix O to describe CA operations.**<br>**4. Added notes to PPDG an iVDGL for termination and transfer to OSG. OSG will be acting as a Catch-all like LCG** |
| **2.9** | **15 Dec 2006 (mwh)** | **1. Added NERSC RA/updates to NERSC disclosure appendix (SC)**<br>**2. Changed Chairman and document contacts** |
| **2.10** | **28 Mar 2008 (mwh)** | **1. ANL disclosure update (JV)**<br>**2. Phillips disclosure (RvD)**<br>**3. Made format consistent to deal with above changes and improve navigation & maintainability in the future** |
| **2.10** | **28 Mar 2008 (jv)** | **4. Format/typo corrections to ANL RA**<br>**5. Clarification of ATO & related** |