DOE Science Grid PKI Certificate Policy

And

Certification Practice Statement

Version 2.1

August 26, 2002

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 used by ESnet to run the DOE Science Grids PKI.

This document will include both the Certificate Policy and the Certification Practice Statement for the DOE Science Grid (DOESG) PKI. The general architecture is a certificate authority with several Registration Authorities. The certificate authority is a subordinate of the ESnet root CA. There is a Registration Authority for each DOESG 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 DOESG PKI are covered in the specific VO or Site Appendixes in this document.

It is the intent of this CA to issue End Entity certificates for use in Grids that are used by DOE researchers. Thus these certificates should be compatible with the Globus middleware that is used on these Grids.

The DOESG PKI will be based on Iplanet CMS running on a Solaris platform. This configuration directly influences the architecture supported.

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, and that are operated by ESnet.

Host Certificate
A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine.

Person Certificate
A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Management Authority (PMA)
For the ESnet/SciGrid CA this is a committee composed of the CA managers and representatives from the site/VO Registration Authorities.

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 DOESG 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 (DOESG) to issue X.509 certificates.

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

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.

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:
DOESG CA Certificate Policy and Certification Practice Statement

Document version:
2.0

Document date:
May 15, 2002.

OID: [ESnet].ERmember.DOEScienceGrid.Security.CP

1.2.840.113612.3.6.4.1

1.3 Community and Applicability

1.3.1 Certification Authorities

ESnet will manage the DOE Science Grid PKI. This is to include the On-line CA and all the Registration Managers located at ESnet data center.

1.3.2 Registration Authorities

ESnet manages the functions of the DOESG Registration Authority under the rules of this CP-CPS. It will also manage the functions of subordinate Registration Authorities, each representing a Virtual Organization (VO) or Site within the ESnet community. Remote Registration managers, those not located at the ESnet Data Center will be incorporated in the DOESG PKI. The Remote Registration Manager is operated by the remote site or VO. That site must comply with the rules and procedure of this CP-CPS. The physical equipment and software are to be managed by the remote site and documented in their Site RA appendix.

1.3.3 End Entities

DOESG 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).

1.3.4 Applicability

See section 1.1.1 for definition of certificate types.

Person certificates can be used to authenticate a person to research sites that have agreed to accept certificates from the DOE Science 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

DOESG PKI is operated by the **ESnet** and managed by a Policy Management Authority. The members of the PMA can be found on the project web site (http://envisage.es.net/pages/doesgpma.htm)

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

Tony J. Genovese

One Cyclotron Road, B50A 3131

Berkeley, CA 94706
phone: +1 510 486 4003
fax: +1 510 486 4790
e-mail: Tony@es.net

2 General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

DOESG CA will:

- Accept certification requests from entitled entities;
- Notify the RA of certification request and accept authentication results from the RA.
- Issue certificates based on the requests from authenticated entities;
- Notify the subscriber of the issuing of the certificate;
- Publish the issued certificates;
- Accept revocation requests according to the procedures outlined in this document;
- Authenticate entities requesting the revocation of a certificate, possibly by delegating this task to a DOESG RA;
- Issue a Certificate Revocation List (CRL);
- Publish the CRL issued.
- Keep audit logs of the certificate issuance process

A DOESG RA will:

- Accept authentication requests from the DOESG CA;
- Authenticate entity making the certification request according to procedures outlined in this document;
- Notify the DOESG CA when authentication is completed for a certification or revocation request;
- Accept revocation requests according to the procedures outlined in this document;
- Notify the DOESG CA of all revocation requests;
- 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.
- Will not approve a certificate with a life time greater then 48 months. Each VO/Site will specify the life time of their certificates in their specific appendix.
- Additional guidelines are described in Appendix A and the individual VO Appendix included in this document.

2.1.2 Subscriber Obligations

Subscribers must:

- Read and adhere to the procedures published in this document;
- Read and adhere to the ESnet Acceptable Use Policy (http://es.net/hypertext/esnet-aup.html)
- Generate a key pair using a trustworthy method;

- 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
        - Storing them encrypted whenever possible.
        - They may be kept unencrypted on the host that they represent.
- Provide correct personal information and authorize the publication of the certificate
- Notify DOESG PKI immediately in case of private key loss or compromise.
- 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 DOESG certificate.

Relying parties may:

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

2.1.4 Repository Obligations

DOESG PKI will provide access to DOESG CA information, as outlined in section 2.6.1, on its web site: http://www.doegrids.org/ca/.

2.2 Liability

DOESG 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.

DOESG PKI and its agents make no guarantee about the security or suitability of a service that is identified by a DOESG 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.

DOESG 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.

2.5 Fees

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

2.6 Publication and Repositories

2.6.1 Publication of CA information

DOESG PKI will operate a secure online repository that contains:

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

2.6.2 Frequency of Publication

- Certificates will be published to the DOESG 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 DOESG 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.

DOESG PKI does not impose any access control on its Policy, its signing Certificate and issued certificates, and its CRLs. In the future, DOESG 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 is at www.doegrids.org/ca/

2.7 Compliance audit

The DOESG PKI will not be 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

DOESG 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.

DOESG PKI does not collect any kind of confidential information.

DOESG PKI does not have access to or generate the private keys of a digital signature key pair, such as those used in DOESG 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] 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 DOESG PKI. Each CN component will include the Full name of the subscriber as determined by the Virtual Organization/Site's RA. Each Common Name will have appended 5 or 6 random alphanumeric characters (i.e. "John K. Doe 1W2D3"). Certificates must apply to unique individuals or resources. Private keys associated with Person certificates may not be hared between people. For Hosts and Services the CN should contain the FQDN of the host.

3.1.4 Method to Prove Possession of Private Key

No stipulation.

3.1.5 Authentication of Individual Identity

ESnet will deploy Registration Managers to each virtual organization and site under DOESG. 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 local 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.

- **Person**.
  Certificate signing requests (CSRs) are submitted by an online procedure, using a Netscape or Internet Explorer browser. The CSR is sent to the VO's or Site's RA for validation. (see Appendices for specific RA).
- **Host or Service**.
  Certificate requests are presented to the VO or Site's RA via a secure method and may come only from valid DOESG certificate holders. The request is sent to the VO or Site RA for validation.

4.2 Certificate Issuance

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

4.3 Certificate Acceptance

No Stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

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 Relaying Parties' resources;
- The subscriber violated his/her obligations.

4.4.2 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 DOESG PKI managers.
- 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.

4.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself to the DOESG PKI or the VO's RA staff, which must use the same procedures used for the authentication of identity of a person.

4.4.4 Circumstances for Suspension

The DOE Science Grid PKI does not support Certificate Suspension.

4.4.5 CRL Issuance Frequency

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

4.4.6 Online Revocation/status checking availability

An online Status checking facility will be provided.

4.4.7 Online Revocation checking requirements

No stipulation.

4.4.8 Other forms of revocation advertisement available

No stipulation.

4.5 Security Audit Procedures

Security Auditing of the DOESG PKI is not supported.

4.6 Records Archival

4.6.1 Types of Event Recorded

The following events are recorded and archived

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

4.6.2 Retention Period for Archives

Minimum retention period is three years.

4.7 Key Changeover

No stipulation.

4.8 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.

4.9 CA Termination

Before DOESG 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.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

The DOESG 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 DOESG PKI managers 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.

The DOESG 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 DOESG PKI is limited to DOESG PKI managers 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. DOESG PKI does not generate private keys.

6.1.2 Private Key Delivery to Entity

The DOESG 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

DOESG certificates may be used only for authentication and signing proxy certificates [Proxy]. They are not recommended for use in non-repudiation, data confidentiality, and message integrity. It is understood that they could be used in this capacity but the DOESG PKI service does not recommend use of or warrant its certificates in this capacity.

The ESnet root CA private key will only be used to sign subordinate CAs. The DOESG online CA signing key is the only key that should be used for signing CRLS and Certificates for Persons, Services. The intention is that certificates issued by the DOESG online CA be capable of signing Proxy Certificates [proxy].

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.

DOESG CA private key is kept, encrypted, in multiple copies and in different locations, on CD-ROMs. For emergencies, the pass phrase is in a sealed envelope kept in a safe. (Reviewing other methods, i.e. FIPS 140 equipment)

6.3 Other Aspects of Key Pair Management

DOESG CA certificate has a validity of **ten** years.

6.4 Activation Data

DOESG CA private key is protected by a pass phrase.

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

The Root Certificate Authority will be off line and will only sign subordinate CAs. DOESG will maintain an Online CA for issuing Certificates authorized by the DOESG RAs.

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

6.8 Cryptographic Module Engineering Controls

No stipulations.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number

X.509 v3.

7.1.2 Certificate Extensions

Basic Constraints (CRITICAL)
not a CA.

Key Usage (CRITICAL)
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

Subject Key Identifier

Authority Key Identifier

Subject Alternative Name
Subject's e-mail address

Issuer Alternative Name

CRL Distribution Points

Certificate Policies

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=Host, is only for internal use of DOESG.

Issuer: DC=doesciencegrid; DC=org; CN=doesg ca;

Or: O= doesciencegrid.org; CN=doesg ca

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; O=doesciencegrid.org
- **For People:** OU=People; DC=doesciencegrid; DC=org
- **For Hosts:** OU=Hosts; O=doesciencegrid.org
- **For Hosts:** OU=Hosts; DC=doesciencegrid; DC=org
- **For Services:** OU=Services; O=doesciencegrid.org
- **For Services:** OU=Services; ; DC=doesciencegrid; 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; O=doesciencegrid.org
  - CN= John K. Doe 1W2D3; OU=People; DC=doesciencegrid; DC=org
- **For a Host**.
  A fully qualified Domain name as registered in DNS, optionally prefixed with "host/".
  - CN= george.lbl.gov; OU=Hosts; O=doesciencegrid.org
- **For a Service**.
  The Service name/A fully qualified Domain name as registered in DNS (FQDN)

(i.e.<SRV>/<FQDN>) note: “host” is an acceptable service name, as for example in Globus gatekeeper certificates.

- CN= FTP/george.lbl.gov; OU=Services; O= doesciencegrid.org
- CN= FTP/george.lbl.gov; OU=Services; DC=doesciencegrid; DC=org
- CN= george.lbl.gov; OU=Services; DC=doesciencegrid; DC=org

7.1.5 Name Constraints

Not supported

7.1.6 Certificate Policy Object Identifier

OID: [ESnet].ERmember.DOEScienceGrid.Security.CP

1.2.840.113612.3.6.4.1

7.1.7 Usage of Policy Constraints Extensions

No stipulated.

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 v1.

Version 1 is required for compatibility with Netscape Communicator.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8 Specification Administration

8.1 Specification Change Procedures

Users will not be warned in advance of changes to DOESG CA’s policy and CPS.

8.2 Publication and Notification Procedures

The policy is available at http://www.envisage.es.net/.

8.3 CPS Approval Procedures

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

Appendix A: Guidelines for Registration Managers, Authorities and Agents

A.1 Background

This set of guidelines is intended to address the types of RMs that will be associated with the ESnet/DOE Science Grid (DOESG) CA, and how Registration Authorities and Agents will operate.

A.2 Guidelines

1. Registration Authorities (RA) or Registration Agents (RAg) will perform all of the functions needed to apply certificate issuance policy to potential CA subscribers. The Registration Manager (RM) then generates and forwards a certificate request to the CA.
2. The PMA will approve the CP for each site/VO that applies for an RM.
3. The RA for each site/VO designates a Point of Contact who automatically becomes a member of the ESnet PMA.
4. The RAgs are, at least during the early adopter phase, also automatically members of the PMA. (Or at least they must be known to the PMA.)
5. The RAg need 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 ESnet signed certificate). This agent has approximately the same role and level of responsibility as the agents in an organization that process computer account request forms and make the decision as to whether to issue and account or not.
6. The community RM is a shared resource. The volume of certificate requests must be limited to 20 per day. There is no limit to the number of certificates that a private RM may request from the CA. The reason for this is the potential RM disruption caused by high system load or high request notification load (which currently goes to all RAs using a Community RM) that would be generated by a high rate of certificate requests.
7. Private RMs should have the following characteristics:
    a. The site/VO must provide a Sun, SPARC system, running Solaris 8
    b. The system must run RM software of a configuration approved by the CA management
    c. Whether ESnet or the private RM operator supplies the RM software is subject to negotiation with Netscape.
    d. The system should be kept in a controlled access machine room, or equivalently secure location
    e. The system should be a “single purpose” system (i.e., only run the RM service
8. RAgs, by policy may not do the following:
    a. Sign CA certificates.
    b. Sign a name space not approved by this policy.
    c. Clone or create new RAgs with out the PMA’s approval.

Appendix B: PPDG RA operational procedures

B.1 Background

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOESG 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.

B.2 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 DOESG 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 DOESG CA.

B.2.2 Point of Contact (POC) with DOESG CA

All necessary communications between the DOESG 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 DOESG 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 DOESG 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 DOESG 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 DOESG CA.

B.4.3 Steps in authentication for certification

B.4.3.1 Person Certificate

1. A person requests a certificate from the DOESG 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 DOESG 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 DOESG CA certifiate.
4. Agent approves request if person has a valid DOESG certificate and rejects request if person does not have a valid DOESG 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 DOESG 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 DOESG 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 DOESG CA.

C.2.2 Point of Contact (POC) with DOESG CA (agent)

All necessary communications between the DOESG 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 DOESG 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 DOESG 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 DOESG 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 DOESG CA.

C.4.3 Steps in authentication for certification

C.4.3.1 Person Certificate

1. A person requests a certificate from DOESG 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 Certificate

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

3. Requesting person sends e-mail signed by a valid DOESG certificate confirming the request.
4. 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.
5. 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 24 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 DOESG 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 DOESG 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 DOESG CA guidelines and also pre-existing NERSC authentication and authorization mechanisms.

D.2.2 Point of Contact (POC) with DOESG CA

All necessary communications between the DOESG 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 DOESG CA PMA.

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.

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 DOESG 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 DOESG CA.

The means of secure communications acceptable are:

- Telephone conversation between members of NERSC RA staff
- Secure digitally signed email between individuals with certificates from DOESG CA.
- Paper documents physically signed and dated by either NERSC RA staff or DOESG CA staff

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 DOESG CA, the request includes the name of NERSC VO who will authenticate the request. (secure means)
2. DOESG CA notifies NERSC RA POC of a certification request. (insecure means)
3. NERSC POC retrieves information of certification request from DOESG CA (secure means).
4. NERSC POC notifies NERSC RA staff member that a request is pending including the name, institution and email of the requester (insecure means)
5. NERSC RA staff informs requestor to contact NERSC account staff for authentication.
6. Individual contacts NERSC account staff for access to NERSC resources.
7. NERSC account staff authenticates individual per existing NERSC authentication policy and mechanisms.
8. NERSC account staff notifies NERSC RA staff member of results of authentication procedure.
9. NERSC RA staff notifies POC that authentication has occurred (insecure means)
10. POC calls NERSC RA staff at telephone number listed in institutional phone book, and verifies status of authentication (secure means)
11. POC notifies DOESG CA of the authentication of the request (secure means)

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. All certificates approved by the NERSC RA will expire yearly on September 30th, regardless of the 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 DOESG 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 DOESG 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 DOESG CA. Additional persons may be appointed to the LBNL RA staff by its current members with the approval of the DOESG CA.

E.2.2 Point of Contact (POC) with DOESG CA

All necessary communications between the DOESG 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 DOESG 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 DOESG activities.

E.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between LBNL RA staff to the DOESG 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 DOESG 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 DOESG CA.

E.4.3 Steps in Authentication for Certification

1. A person requests a certificate from DOESG CA, the request includes the name of a LBNL RA staff who can authenticate the request. (secure means)
2. DOESG CA notifies LBNL RA POC of a certification request. (insecure means)
3. POC retrieves information of certification request from DOESG 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 DOESG 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

One of the Virtual Organization Registration Authorities (VO RA) operating with some delegated authority of the DOESG CA is the Oak Ridge National Laboratory (ORNL) Registration Authority (ORNL RA). Information defining the ORNL VO is available at http://www.ornl.gov/. This appendix describes how the responsibilities for a VO RA are implemented for the ORNL RA.

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.

It is expected that the ORNL RA will have a finite lifetime and is implemented as an example of a VO RA for access to ORNL resources. The ORNL RA is subjected to review by local account and resource management authorities during its initial implementation; however, 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 DOESG 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 DOESG CA guidelines and existing ORNL authentication and authorization mechanisms. Additional persons may be appointed to the DOESG RA staff by ORNL and approved by the DOESG 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 DOESG CA

All necessary communications between the DOESG 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 DOESG CA PMA.

F.3 ORNL VO Community

The ORNL Virtual Organization community is defined as all persons who are authorized to utilize ORNL resources. These persons must also follow the *most recent* ORNL usage rules and export control 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

Authentication of an individual identity must strictly follow ORNL usage rules and export control policies. Persons requesting certification are required to have user accounts at ORNL and demonstrate reasonable evidence of membership in the ORNL VO. All individuals must apply for ORNL accounts if they do not already have ones. In the application process, the individuals will have to list a project affiliation and give a general description of work being performed. This is to assure that ORNL resources are not being used for unauthorized purposes.

After getting accounts, the individuals must inform the ORNL RA staff of their project affiliation, and names of the PI and system administrators who are responsible for their account creations. The ORNL RA will contact the PI and system administrators to verify the individuals' rights to access ORNL resources.

F.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between ORNL RA staff to the DOESG 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 DOESG 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 DOESG CA
- Paper documents physically signed and dated by either ORNL RA staff or DOESG 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

1. Individual requests a certificate from DOESG CA, the request includes the name of ORNL RA who will authenticate the request. (secure means)
2. DOESG CA notifies ORNL RA POC of a certification request. (insecure means)
3. ORNL POC retrieves information of certification request from DOESG CA (secure means).
4. ORNL POC notifies ORNL RA staff member that a request is pending including the name, institution and email of the requester (insecure means)
5. ORNL RA staff informs requestor to apply for an ORNL account on-line if the requestor does not have one. The ORNL RA staff will skip step 6 if the requestor already has an account.
6. The ORNL account staff will review the account request and email the requestor of its disposition. The decision will be made based on existing ORNL authentication and authorization policies.
7. If the account is granted, the requestor has to inform ORNL RA staff of his/her affiliated project, and names of PI and system administrators who are responsible for account creation.
8. ORNL RA staff contact the PI and the system administrator to verify the requestor's authentication and authorization to access ORNL resources.
9. ORNL RA staff notifies POC that authentication has occurred (insecure means)
10. POC calls ORNL RA staff at telephone number listed in institutional phone book, and verifies status of authentication (secure means)
11. POC notifies DOESG CA of the authentication of the request (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) DOESG 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 ANL RA is subjected to review by local account and resource management authorities.

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 DOESG. These persons have been designated by ANL and are ANL staff members.

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

G.2.2 Point of Contact (POC) with DOESG CA

All necessary communications between the DOESG 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 DOESG CA PMA.

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 DOESG 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 DOESG 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 DOESG CA
- Paper documents physically signed and dated by either ANL RA staff or DOESG CA staff

G.4.3 Steps in authentication for certification

1. Individual requests a certificate from DOESG 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. DOESG 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 DOESG CA (secure means).
4. ANL RA staff contact the requestor and verifies the requestor's identity.
5. If the subscriber is successfully vetted, ANL RA staff approves certificate request (secure means).

G.5 Lifetime of certificates

Certificates will be valid for two years.

Appendix H: PNNL RA operational procedures

H.1 Background

The Pacific Northwest National Laboratory (PNNL) DOESG 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 DOESG. 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 DOESG CA guidelines and existing PNNL authentication and authorization mechanisms. Additional persons may be appointed to the DOESG RA staff by PNNL.

H.2.2 Point of Contact (POC) with DOESG CA

All necessary communications between the DOESG 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 DOESG 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 DOESG 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 DOESG 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 DOESG CA
- Paper documents physically signed and dated by either PNNL RA staff or DOESG CA staff

H.4.3 Steps in authentication for certification

1. Individual requests a certificate from DOESG 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. DOESG 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 DOESG 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 30th of each year.

Appendix I: iVDGL RA operational procedures

I.1 Purpose, Goals, Scope

One of the Virtual Organizations Registration Authorities (VO RA) operating with some delegated authority of the DOESG 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 a VO RA are implemented for the iVDGL RA. 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 may be extended to other application and experiment groups, through MOUs. The iVDGL VO 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 (www.ivdgl.org/TBD). Each of these persons has a valid certificate from the DOESG 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 DOESG certificates.

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

I.2.2 POC with DOESG CA

All necessary communications between the DOESG 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 DOESG 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 VO.

I.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between iVDGL RA staff to the DOESG 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 DOESG 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 DOESG CA.

I.4.3 Steps in authentication for certification

1. A person requests a certificate from DOESG CA; the request includes the name of an iVDGL RA staff member that can authenticate the request. (Secure means)
2. DOESG CA notifies iVDGL RA agents of a certification request. (Insecure means)
3. Agent retrieves information of certification request from DOESG CA. (Secure means)
4. 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)
5. iVDGL RA staff (sponsor) contacts requester and authenticates request (secure means).
6. iVDGL RA staff notifies agent that authentication has occurred (secure means)
7. Agent notifies DOESG CA of the authentication of the request (secure means)

I.5 Lifetime of certificates

Identity certificates approved by the iVDGL RA have a lifetime of no more than 24 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 DOESG 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 DOESG CA.

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

J.2.2 Point of Contact (POC) with DOESG CA

All necessary communications between the DOESG 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 DOESG 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 DOESG 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 DOESG 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 DOESG CA.

J.4.3 Steps in authentication for certification

J.4.3.1 Person Certificate

1. A person requests a certificate from the DOESG 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 retrives notification of certificate request from DOESG 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 occured. (secure means)
7. Agent notifies DOESG CA of the autehtication 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 servcie certificate from the DOESG 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 DOESG CA certifiate.
4. Agent approves request if person has a valid DOESG certificate and rejects request if person does not have a valid DOESG 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.

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/

[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 DOESG PMA responsibility for CP/CPS maintenance Section 2.1: Split CA and RA obligations

		Section 3.1.1/7.1.4: Changed host name requirement - Von Welch's text added Section 4.2: Added certificate life cycle text Section 4.4: Did a little more on Revocation process/reasons. Added RA support, including Appendixes for PPDG, FNC and RA guidelines. Redid format and reviewed/rewrote all sections of the CP-CPS
2.0	May 15, 2002	Numerous modifications to text based on input from PMA
2.1	Aug 26, 2002	Add iVDGL and ESG appendixes