



DOEGrids CA Certificate Policy and Certification Practice Statement

Version 3.1

Editors:
Michael Helm
Victoria Elliott
Dhiva Muruganantham
Doug Olson
Dan Peterson
John Volmer



TABLE OF CONTENTS

1. INTRODUCTION	1
1.1. Overview	1
1.2. Document Name and Identification	2
1.3. PKI Participants	3
1.3.1. Certification Authorities	3
1.3.2. Registration Authorities	5
1.3.3. Subscribers (End Entities)	6
1.3.4. Relying Parties	7
1.3.5. Other Participants	7
1.4. Certificate Usage	8
1.4.1. Appropriate Certificate Uses	8
1.4.2. Prohibited Certificate Uses	8
1.5. Policy Administration	8
1.5.1. Organization Administering the Document	9
1.5.2. Contact Person	9
1.5.3. Person Determining CPS Suitability for the Policy	10
1.5.4. CPS Approval Procedures	10
1.6. Definitions and Acronyms	10
1.6.1. Definitions	14
1.6.2. Acronyms	14
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	15
2.1. Repositories	15
2.2. Publication of Certification Information	16
2.3. Time or Frequency of Publication	16
2.4. Access Controls on Repositories	16
3. IDENTIFICATION AND AUTHENTICATION	17
3.1. Naming	17
3.1.1. Types of Names	17
3.1.2. Need for Names to be Meaningful	17
3.1.3. Anonymity or Pseudonymity of Subscribers	18
3.1.4. Rules for Interpreting Various Name Forms	18
3.1.5. Uniqueness of Names	18
3.1.6. Recognition, Authentication, and Role of Trademarks	18
3.2. Initial Identity Validation	18
3.2.1. Method to Prove Possession of Private Key	18
3.2.2. Authentication of Organization Identity	19
3.2.3. Authentication of Individual Identity	19
3.2.4. Non-Verified Subscriber Information	20
3.2.5. Validation of Authority	20
3.2.6. Criteria for Interoperation	20
3.3. Identification and Authentication for Re-key Requests	20
3.3.1. Identification and Authentication for Routine Re-key	20
3.3.2. Identification and Authentication for Re-key after Revocation	21
3.4. Identification and Authentication for Revocation Request	21
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	23

4.1.	Certificate Application	23
4.1.1.	Who Can Submit a Certificate Application	23
4.1.2.	Enrollment Process and Responsibilities	23
4.2.	Certificate Application Processing	24
4.2.1.	Performing Identification and Authentication Functions	24
4.2.2.	Approval or Rejection of Certificate Applications	24
4.2.3.	Time to Process Certificate Applications	24
4.3.	Certificate Issuance	24
4.3.1.	CA Actions during Certificate Issuance	24
4.3.2.	Notification to Subscriber by the CA of Issuance of Certificate	25
4.4.	Certificate Acceptance	25
4.4.1.	Conduct Constituting Certificate Acceptance	25
4.4.2.	Publication of the Certificate by the CA	25
4.4.3.	Notification of Certificate Issuance by the CA to Other Entities	25
4.5.	Key Pair and Certificate Usage	25
4.5.1.	Subscriber Private Key and Certificate Usage	25
4.5.2.	Relying Party Public Key and Certificate Usage	26
4.6.	Certificate Renewal	26
4.6.1.	Circumstance for Certificate Renewal	26
4.6.2.	Who May Request Renewal	26
4.6.3.	Processing Certificate Renewal Requests	27
4.6.4.	Notification of New Certificate Issuance to Subscriber	27
4.6.5.	Conduct Constituting Acceptance of a Renewal Certificate	27
4.6.6.	Publication of the Renewal Certificate by the CA	27
4.6.7.	Notification of Certificate Issuance by the CA to Other Entities	27
4.7.	Certificate Re-key	27
4.7.1.	Circumstance for Certificate Re-key	27
4.7.2.	Who May Request Certification of a New Public Key	28
4.7.3.	Processing Certificate Re-keying Requests	28
4.7.4.	Notification of New Certificate Issuance to Subscriber	28
4.7.5.	Conduct Constituting Acceptance of a Re-keyed Certificate	28
4.7.6.	Publication of the Re-keyed Certificate by the CA	28
4.7.7.	Notification of Certificate Issuance by the CA to Other Entities	28
4.8.	Certificate Modification	28
4.8.1.	Circumstances for Certificate Modification	28
4.8.2.	Who May Request Certificate Modification	28
4.8.3.	Processing Certificate Modification Requests	29
4.8.4.	Notification of New Certificate Issuance to Subscriber	29
4.8.5.	Conduct Constituting Acceptance of Modified Certificate	29
4.8.6.	Publication of the Modified Certificate by the CA	29
4.8.7.	Notification of Certificate Issuance by the CA to Other Entities	29
4.9.	Certificate Revocation and Suspension	29
4.9.1.	Circumstances for Revocation	29
4.9.2.	Who Can Request Revocation	30
4.9.3.	Procedure for Revocation Request	30
4.9.4.	Revocation Request Grace Period	31

4.9.5.	Time Within Which CA Must Process the Revocation Request.....	31
4.9.6.	Revocation Checking Requirement for Relying Parties.....	31
4.9.7.	CRL Issuance Frequency (if applicable).....	31
4.9.8.	Maximum Latency for CRLs (if applicable).....	31
4.9.9.	Online Revocation/Status-Checking Availability.....	31
4.9.10.	Online Revocation Checking Requirements.....	31
4.9.11.	Other Forms of Revocation Advertisements Available.....	32
4.9.12.	Special Requirements Re-key Compromise.....	32
4.9.13.	Circumstances for Suspension.....	32
4.9.14.	Who Can Request Suspension.....	32
4.9.15.	Procedure for Suspension Request.....	32
4.9.16.	Limits on Suspension Period.....	32
4.10.	Certificate Status Services.....	32
4.10.1.	Operational Characteristics.....	33
4.10.2.	Service Availability.....	33
4.10.3.	Optional Features.....	33
4.11.	End of Subscription.....	33
4.12.	Key Escrow and Recovery.....	33
4.12.1.	Key Escrow and Recovery Policy and Practices.....	33
4.12.2.	Session Key Encapsulation and Recovery Policy and Practices.....	33
5.	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	35
5.1.	Physical Controls.....	35
5.1.1.	Site Location and Construction.....	35
5.1.2.	Physical Access.....	35
5.1.3.	Power and Air Conditioning.....	36
5.1.4.	Water Exposures.....	36
5.1.5.	Fire Prevention and Protection.....	36
5.1.6.	Media Storage.....	36
5.1.7.	Waste Disposal.....	36
5.1.8.	Off-Site Backup.....	36
5.2.	Procedural Controls.....	36
5.2.1.	Trusted Roles.....	36
5.2.2.	Number of Persons Required per Task.....	37
5.2.3.	Identification and Authentication for Each Role.....	37
5.2.4.	Roles Requiring Separation of Duties.....	37
5.3.	Personnel Controls.....	37
5.3.1.	Qualifications, Experience, and Clearance Requirements.....	37
5.3.2.	Background Check Procedures.....	37
5.3.3.	Training Requirements.....	37
5.3.4.	Retraining Frequency and Requirements.....	38
5.3.5.	Job Rotation Frequency and Sequence.....	38
5.3.6.	Sanctions for Unauthorized Actions.....	38
5.3.7.	Independent Contractor Requirements.....	38
5.3.8.	Documentation Supplied to Personnel.....	38
5.4.	Audit Logging Procedures.....	38
5.4.1.	Types of Events Recorded.....	38

5.4.2.	Frequency of Processing Log	39
5.4.3.	Retention Period for Audit Log	39
5.4.4.	Protection of Audit Log	39
5.4.5.	Audit Log Backup Procedures	39
5.4.6.	Audit Collection System (Internal vs. External).....	39
5.4.7.	Notification to Event-Causing Subject	40
5.4.8.	Vulnerability Assessments.....	40
5.5.	Records Archival	40
5.5.1.	Types of Records Archived	40
5.5.2.	Retention Period for Archive.....	40
5.5.3.	Protection of Archive	40
5.5.4.	Archive Backup Procedures	41
5.5.5.	Requirements for Time-Stamping of Records	41
5.5.6.	Archive Collection System (Internal or External)	41
5.5.7.	Procedures to Obtain and Verify Archive Information.....	41
5.6.	Key Changeover.....	41
5.7.	Compromise and Disaster Recovery	41
5.7.1.	Incident and Compromise Handling Procedures	42
5.7.2.	Computing Resources, Software, and/or Data Are Corrupted.....	42
5.7.3.	Entity Private Key Compromise Procedures.....	42
5.7.4.	Business Continuity Capabilities After a Disaster	42
5.8.	CA or RA Termination.....	42
6.	TECHNICAL SECURITY CONTROLS.....	45
6.1.	Key Pair Generation and Installation	45
6.1.1.	Key Pair Generation	45
6.1.2.	Private Key Delivery to Subscriber	45
6.1.3.	Public Key Delivery to Certificate Issuer.....	46
6.1.4.	CA Public Key Delivery to Relying Parties.....	46
6.1.5.	Key Sizes	46
6.1.6.	Public Key Parameters Generation and Quality Checking	46
6.1.7.	Key Usage Purposes (as per X.509 v3 key usage field).....	47
6.2.	Private Key Protection and Cryptographic Module Engineering Controls	
	47	
6.2.1.	Cryptographic Module Standards and Controls.....	47
6.2.2.	Private Key (n out of m) Multi-Person Control	48
6.2.3.	Private Key Escrow	48
6.2.4.	Private Key Backup	48
6.2.5.	Private Key Archival	48
6.2.6.	Private Key Transfer into or from a Cryptographic Module.....	48
6.2.7.	Private Key Storage on Cryptographic Module.....	49
6.2.8.	Method of Activating Private Key.....	49
6.2.9.	Method of Deactivating Private Key.....	49
6.2.10.	Method of Destroying Private Key.....	49
6.2.11.	Cryptographic Module Rating	49
6.3.	Other Aspects of Key Pair Management	49
6.3.1.	Public Key Archival.....	50

6.3.2.	Certificate Operational Periods and Key Pair Usage Periods.....	50
6.4.	Activation Data	50
6.4.1.	Activation Data Generation and Installation.....	51
6.4.2.	Activation Data Protection	51
6.4.3.	Other Aspects of Activation Data.....	51
6.5.	Computer Security Controls.....	51
6.5.1.	Specific Computer Security Technical Requirements.....	51
6.5.2.	Computer Security Rating	51
6.6.	Lifecycle Technical Controls	52
6.6.1.	System Development Controls	52
6.6.2.	Security Management Controls	52
6.6.3.	Lifecycle Security Controls	52
6.7.	Network Security Controls	52
6.8.	Time-Stamping	52
7.	CERTIFICATE, CRL, AND OCSP PROFILES.....	54
7.1.	Certificate Profile	54
7.1.1.	Version Number(s)	54
7.1.2.	Certificate Extensions.....	54
7.1.3.	Algorithm Object Identifiers	56
7.1.4.	Name Forms.....	56
7.1.5.	Name Constraints.....	57
7.1.6.	Certificate Policy Object Identifier.....	57
7.1.7.	Usage of Policy Constraints Extension.....	57
7.1.8.	Policy Qualifiers Syntax and Semantics	57
7.1.9.	Processing Semantics for the Critical Certificate Policies Extension	57
7.2.	CRL Profile	57
7.2.1.	CRL and CRL Entry Extensions	58
7.3.	Online Certificate Status Protocol (OCSP) Profile	58
7.3.1.	Version Number(s)	59
7.3.2.	OCSP Extensions.....	59
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	60
8.1.	Frequency or Circumstances of Assessment	60
8.2.	Identity/Qualifications of Assessor.....	60
8.3.	Assessor's Relationship to Assessed Entity	60
8.4.	Topics Covered by Assessment	60
8.5.	Actions Taken as a Result of Deficiency.....	60
8.6.	Communication of Results.....	61
9.	OTHER BUSINESS AND LEGAL MATTERS.....	62
9.1.	Fees	62
9.1.1.	Certificate Issuance or Renewal Fees	63
9.1.2.	Certificate Access Fees.....	63
9.1.3.	Revocation or Status Information Access Fees.....	63
9.1.4.	Fees for Other Services.....	63
9.1.5.	Refund Policy	63
9.2.	Financial Responsibility	63

9.2.1.	Insurance Coverage	63
9.2.2.	Other Assets.....	63
9.2.3.	Insurance or Warranty Coverage for End Entities	64
9.3.	Confidentiality of Business Information.....	64
9.3.1.	Scope of Confidential Information	64
9.3.2.	Information Not Within the Scope of Confidential Information	64
9.3.3.	Responsibility to Protect Confidential Information	64
9.4.	Privacy of Personal Information.....	64
9.4.1.	Privacy Plan	65
9.4.2.	Information Treated as Private	65
9.4.3.	Information not Deemed Private.....	65
9.4.4.	Responsibility to Protect Private Information.....	65
9.4.5.	Notice and Consent to Use Private Information.....	65
9.4.6.	Disclosure Pursuant to Judicial or Administrative Process	65
9.4.7.	Other Information Disclosure Circumstances	66
9.5.	Intellectual Property Rights.....	66
9.6.	Representations and Warranties	66
9.6.1.	CA Representations and Warranties	66
9.6.2.	RA Representations and Warranties	66
9.6.3.	Subscriber Representations and Warranties.....	67
9.6.4.	Relying Party Representations and Warranties.....	67
9.6.5.	Representations and Warranties of Other Participants.....	67
9.7.	Disclaimers of Warranties.....	67
9.8.	Limitations of Liability.....	67
9.9.	Indemnities	67
9.10.	Term and Termination.....	68
9.10.1.	Term	68
9.10.2.	Termination.....	68
9.10.3.	Effect of Termination and Survival	68
9.11.	Individual Notices and Communications with Participants	68
9.12.	Amendments.....	69
9.12.1.	Procedure for Amendment.....	70
9.12.2.	Notification Mechanism and Period.....	70
9.12.3.	Circumstances Under Which OID Must Be Changed.....	70
9.13.	Dispute Resolution Provisions	70
9.14.	Governing Law.....	70
9.15.	Compliance with Applicable Law.....	71
9.16.	Miscellaneous Provisions.....	71
9.16.1.	Entire Agreement	71
9.16.2.	Assignment	71
9.16.3.	Severability	71
9.16.4.	Enforcement (Attorneys' Fees and Waiver of Rights)	71
9.16.5.	Force Majeure.....	71
9.17.	Other Provisions	72
10.	COMPLIANCE WITH THE CA CLASSIC PROFILE	73
1.	Section 1	73

2.	General Architecture	73
3.	Identity	73
4.	Operational Requirements	75
5.	Site Security	77
6.	Publication and Repository Responsibilities	77
7.	Audits	78
8.	Privacy and Confidentiality	78
9.	Compromise and Disaster Recovery	79
11.	REFERENCES	81
12.	ACKNOWLEDGMENTS	83
	LIST OF CHANGES	85
	Appendix A: General Guidelines for DOEGrids Registration Authorities, Agents, and Grid Administrators	87
A.1	Background	87
A.2	Guidelines	87
A.3	Agreements for Registration Authority, Agents and Grid Administrators (GridAdmins)	88
A.3.1	RA declaration to DOEGrids PMA	88
A.3.2	Letter Requesting Assignment of RA Agent Role	89
A.3.3	Letter Requesting RA Agent Role	89
A.3.4	Grid Administrators	90
	Appendix B: PPDG RA Operational Procedures	91
B.1	Background	91
B.2.1	Membership	91
B.2.2	Point of Contact (POC) with DOEGrids CA	91
B.3	PPDG VO Community	91
B.4	Authentication Procedures	91
B.4.1	Authentication of Individual Identity	91
B.4.2	Communications	92
B.4.3	Steps in Authentication for Certification	92
B.4.3.1	Person Certificate	92
B.4.3.2	Host or Service Certificate	92
	Appendix C: National Fusion Collaboratory's RA Operational Procedures	93
C.1	Purpose, Goals, Scope	93
C.2	NFC RA Staff (sponsors)	93
C.2.1	Membership	93
C.2.2	Point of Contact (POC) with DOEGrids CA (agent)	93
C.3	NFC VO Community	93
C.4	Authentication Procedures	94
C.4.1	Authentication of Individual Identity	94
C.4.2	Communications	94
C.4.3	Steps in Authentication for Certification	94
C.4.3.1	Person Certificate	94
C.4.3.2	Host or Service Certificate	94
	Appendix D: NERSC RA Operational Procedures	96
D.1	Background	96

D.2 NERSC RA Staff	96
D.2.1 Membership	96
D.2.2 Point of Contact (POC) with DOEGrids CA	96
D.3 NERSC VO Community	97
D.4 Authentication Procedures.....	97
D.4.1 Authentication of Individual Identity	97
D.4.2 Communications	97
D.4.3 Steps in Authentication for Certification.....	98
Appendix E: Lawrence Berkeley Lab’s RA Operational Procedures.....	99
E.1 Purpose, Goals and Scope	99
E.2 VO RA staff	99
E.2.1 Membership.....	99
E.2.2 Point of Contact (POC) with DOEGrids CA	99
E.3 LBNL Site Community.....	99
E.4 Authentication Procedures.....	99
E.4.1 Authentication of Individual Identity	99
E.4.2 Communications.....	100
E.4.3 Steps in Authentication for Certification.....	100
Appendix F: ORNL RA Operational Procedures	101
F.1 Background	101
F.2 ORNL RA staff	101
F.2.1 Membership.....	101
F.2.2 Point of Contact (POC) with DOEGrids CA	101
F.3 ORNL Community	101
F.4 Authentication Procedures	102
F.4.1 Authentication of Individual Identity	102
F.4.2 Communications.....	102
F.4.3 Steps in Authentication for Certification	102
Appendix G: ANL RA Operational Procedures.....	104
G.1 Background	104
G.2 ANL RA staff.....	104
G.2.1 Membership	104
G.2.2 Point of Contact (POC) with DOEGrids CA.....	105
G.2.3 Authentication to DOEGrids CA	105
G.2.4 Communication with DOEGrids CA	105
G.3 ANL Community	105
G.4 Authentication Procedures.....	106
G.4.1 Authentication of Individual Identity.....	106
G.4.2 Communications	106
G.4.3 Steps in Authentication for Certification	106
Appendix H: PNNL RA Operational Procedures	107
H.1 Background.....	107
H.2 PNNL RA staff	107
H.2.1 Membership	107
H.2.2 Point of Contact (POC) with DOEGrids CA.....	107
H.3 PNNL Community	107

H.4 Authentication Procedures.....	108
H.4.1 Authentication of Individual Identity.....	108
H.4.2 Communications	108
H.4.3 Steps in Authentication for Certification.....	108
H.5 Lifetime of Certificates.....	108
Appendix I: iVDGL RA Operational Procedures.....	109
I.1 Purpose, Goals, Scope	109
I.2 iVDGL RA staff (sponsors).....	109
I.2.1 Membership.....	109
I.2.2 POC with DOEGrids CA.....	109
I.3 iVDGL VO Community	109
I.4 Authentication Procedure	110
I.4.1 Authentication of Individual Identity	110
I.4.2 Communications	110
I.4.3 Steps in authentication for personal certification.....	110
I.4.4 Steps in authentication for host/service certification	110
Appendix J: ESG RA Operational Procedures	111
J.1 Background	111
J.2 ESG RA staff	111
J.2.1 Membership	111
J.2.2 Point of Contact (POC) with DOEGrids CA.....	111
J.3 ESG VO Community.....	111
J.4 Authentication Procedures.....	112
J.4.1 Authentication of Individual Identity.....	112
J.4.2 Communications	112
J.4.3 Steps in Authentication for Certification	112
J.4.3.1 Person Certificate	112
J.4.3.2 Host or Service Certificate	112
Appendix K: FNAL RA Operational Procedures.....	114
K.1 Background.....	114
K.2 FNAL RA staff.....	114
K.2.1 Membership.....	114
K.2.2 Point of Contact (POC) with DOEGrids CA	114
K.3 FNAL Community.....	114
K.4 Authentication Procedures.....	114
K.4.1 Authentication of Individual Identity	114
K.4.2 Communications.....	115
K.4.3 Steps in Authentication for Certification.....	115
K.4.3.1 Interactive Method.....	115
K.4.3.2 Batch Method	115
APPendix I: Guidelines for Security Incident Response and Resolution ..	116
L.1 Background	116
L.2 Definitions.....	116
L.3 Responsibilities	116
L.4 Actions	117
Appendix M: LCG RA Operational Procedures	118

M.1 Background	118
M.2 LCG RA Staff.....	118
M.2.1 Membership	118
M.2.2 Point of Contact (POC) with DOEGrids CA.....	118
M.3 LCG RA VO Community.....	118
M.4 Authentication Procedures	119
M.4.1 Authentication of Individual Identity	119
M.4.2 Communications	119
M.4.3 Steps in Authentication for Certification	119
Appendix N: Open Science Grid (OSG) RA Operational Procedures.....	120
N.1 Background.....	120
N.2 OSG RA staff.....	121
N.2.1 Membership	121
N.2.2 Point of Contact (POC) with DOEGrids CA.....	121
N.3 OSG Community.....	121
N.4 Authentication Procedures.....	121
N.4.1 Authentication of Individual Identity	121
N.4.2 Communications	122
N.4.3 Steps in Authentication for Certification.....	123
N.4.3.1 Person Certificate.....	123
N.4.3.2 Service Certificate	123
N.4.4 Logging	123
N.5 Revocation Procedures	124
N.6 Cyber Protection Plan.....	124
Appendix O: General Guidelines for DOEGrids CA Operations	125
This Appendix has been superseded by ESnet RA Operational Procedures, Appendix Q.	125
O.1 Background	125
O.2 CA Operations Staff.....	125
O.3 CA Operations	125
Appendix P: Philips Research (US) RA Operational Procedures	127
P.1 Background.....	127
P.2 Philips Research (US) RA Staff	127
P.2.1 Membership.....	127
P.2.2 Point of Contact (POC) with DOEGrids CA	127
P.3 Philips Research (US) Community.....	128
P.4 Authentication Procedures	128
P.4.1 Authentication of Individual Identity	128
P.4.2 Communications.....	128
P.4.3 Steps in Authentication for Certification.....	129
Appendix Q: ESnet RA Operational Procedures.....	130
Q.1 Background	130
Q.2 ESnet RA Staff	130
Q.2.1 Membership	130
Q.2.2 Point of Contact (POC) with DOEGrids CA.....	131
Q.2.3 Communication with DOEGrids CA	131

Q.3 ESnet Community.....	131
Q.4 Authentication Procedures.....	131
Q.4.1 Authentication of Individual Identity.....	131
Q.4.2 Communications	131
Q.4.3 Steps in Authentication for Certification	131
Q.5 DOEGrids CA Operations.....	132

1. INTRODUCTION

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the CP or the CPS being written) is targeted.

This document follows the framework and structure outlined in the Internet Engineering Task Force's RFC 3647 [Chokhani03]. Extracts of this document have been included in this document in a blue font to assist the reader in understanding the certificate policies and certification practice statements. Compliance of this document with the current minimum requirements of the International Grid Trust Federation (IGTF) Classic CA profile [CCA06] is highlighted in Section 10.

Entries in black type represent text translated from DOEGrids v2.10 and used in v3.0. Any changes to the text in v3.0 are indicated by green type.

See the References section at the end of the document for links to source documents.

1.1. Overview

This subcomponent provides a general introduction to the document being written. This subcomponent can also be used to provide a synopsis of the PKI to which the CP or CPS applies. For example, it may set out different levels of assurance provided by certificates within the PKI. Depending on the complexity and scope of the particular PKI, a diagrammatic representation of the PKI might be useful here.

This document is structured according to [RFC3647]. Not all sections of RFC 3647 are used. Sections that are not included have a default value of "No stipulation."

This document is both the Certificate Policy (CP) and the Certification Practice Statement (CPS) for the DOEGrids Certification Authority (CA) and Public Key Infrastructure (PKI). It describes the set of rules and procedures established by the DOEGrids Policy Management Authority (PMA) for the operation of the DOEGrids (PKI) service. The DOEGrids PMA is responsible for this document.

ESnet operates the DOEGrids CA under the authority of the DOEGrids PMA. ESnet headquarters are located at Lawrence Berkeley National Laboratory (LBNL) in Berkeley, California. LBNL and ESnet own and operate the CA and are ultimately responsible to the University of California and the US Department of Energy for the Certification Authority equipment, data, and operations.

The general architecture is a certification authority (CA) with multiple Registration Authorities. The DOEGrids CA is a subordinate of the ESnet root CA. There is a Registration Authority for each DOEGrids site or Virtual Organization (VO). Each Registration Authority is responsible for verifying user identities of its community. Special guidelines for the individual RAs of the DOEGrids PKI are covered in the specific Registration Authority Appendices in this document.

DOEGrids CA is a Traditional X.509 Public Key Certification Authority that complies with the International Grid Trust Federation (IGTF) "Profile for Classic X.509 Public Key Certification Authorities with secure infrastructure." The DOEGrids CA issues personal and service certificates for use in Grids. These certificates are for DOE researchers and their colleagues. These certificates are compatible with the middleware that is used on these Grids.

The DOEGrids personal certificates by themselves should not to be used to determine authorization. The DOEGrids personal certificate should be used only to assert the identity of the individual named in the personal certificate. Authorization decisions should be based on criteria other than the DOEGrids personal certificate.

RFC 2527: §1.1

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.1

1.2. Document Name and Identification

This subcomponent provides any applicable names or other identifiers, including ASN.1 object identifiers, for the document. An example of such a document name would be the US Federal Government Policy for Secure E-mail.

Document title: DOEGrids CA Certificate Policy and Certification Practice Statement

Document version: 3.1

Document date: July 30, 2009

OID: [ESnet].ERmember.DOEGrids.CP-CPS.CPVersionNumber.CPReleaseNumber
1.2.840.113612.3.7.1.3.1

The next table describes the meaning of the OID:

1.2.840	Prefix for US ANSI registrants Iso(1) member-body(2) us(840)
113612	Energy Sciences Network (ESnet)
3	ERmember
7	DOEGrids
1	DOEGrids CP/CPS
3.1	Major and minor CP/CPS version number

This OID assignment can be verified here:

<http://www.es.net/OID/ESnet-OID-list.txt>

and (in part) here:

<http://www.oid-info.com/get/1.2.840.113612>

It may be possible to verify the organization name registration “Energy Sciences Network” directly with ANSI. Contact ANSI (<http://ansi.org>) and search for “Registration Programs.”

RFC 2527: §1.2

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.2

1.3. PKI Participants

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI.

All RA, agents, and subscribers are 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 e-mail address
2. Name
3. End entity is 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
 - Are responsible for the day-to-day operations of the CA.
 - Have the authority to issue and revoke certificates as needed to run the service.
- Registration Authority
 - Is responsible for verifying end entity 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 administrators. Appendix O has details for CA operations.

RFC 2527: §1.3

IGTF Classic: §1 (general)

DOEGrids v2.10: §2.1

1.3.1. Certification Authorities

The entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization’s CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization.

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 Certification Management Service is by a Web browser. Web browsers or other client software are 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.
DOEGrids CA	ESnet Data Center	Signs subscriber, host and Service Certificates.
DOEGrids Community Registration Manager (RM)	ESnet Data Center	Creates Certificate Signed Requests that agents use to approve certificate requests.
DOEGrids Lightweight Directory Access Protocol (LDAP) directory	ESnet Data Center	The DOEGrids CA publishes certificates and other information to the directory. The directory is public and read-only.
Subscriber Web browsers	Subscriber desktops	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.

[RFC 2527: §1.3.1](#)

[IGTF Classic: §1 \(general\)](#)

[DOEGrids v2.10: §1.3.1](#)

DOEGrids 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 e-mail 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 DOEGrids 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.

[RFC 2527: §1.3.1](#)

[IGTF Classic: §1 \(general\)](#)

[DOEGrids v2.10: §2.1.1](#)

1.3.2. Registration Authorities

The entities that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.

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

- Approve or reject the certificate request
- Initiate certificate revocations
- Search for certificates.

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

A DOEGrids RA will:

1. Accept authentication requests from the DOEGrids CA;
2. Authenticate the 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 the entity making the request is the registered owner if the DN existed previous to this request and resolve conflicts or manage transfer of DN ownership;
5. Notify the DOEGrids 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 DOEGrids CA of all revocation requests;
8. Authenticate the entity making the 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 than 12 months. Each VO/site will specify the life time of its certificate in its 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 the incident.

13. Publish contact information for the RA;
14. Notify the CA whenever the contact information for the RA changes.

RFC 2527: §1.3.2/1/4

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.3.2/2.1.1

1.3.3. Subscribers (End Entities)

Examples of subscribers who receive certificates from a CA include employees of an organization with its own CA, banking or brokerage customers, organizations hosting e-commerce sites, organizations participating in a business-to-business exchange, and members of the public receiving certificates from a CA issuing certificates to the public at large.

DOEGrids 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 Acceptable Usage Policies (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.

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

- a. Selecting a pass phrase of at minimum **twelve** characters;
- b. Protecting the pass phrase from others;
- c. Always using the pass phrase to encrypt the stored private key;
- d. Never sharing the private key with other users.

For Service Certificates

- a. Storing them encrypted whenever possible;
- b. They may be kept unencrypted on the host that they represent;
- c. Asserting that they are authorized to run install the specified service on the specified host;
- d. Providing correct personal information and authorizing the publication of the certificate;
- e. Verifying that the Distinguished Name (DN) being requested does not yet exist, or asserting that they are the registered owner of the DN.
- f. Notifying DOEGrids PKI immediately of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of the incident.

- g. Use the certificates for the permitted uses only.

RFC 2527: §1.3.3

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.3.3, 2.1.2

1.3.4. Relying Parties

Examples of relying parties include employees of an organization having its own CA who receive digitally signed e-mails from other employees, persons buying goods and services from e-commerce sites, organizations participating in a business-to-business exchange who receive bids or orders from other participating organizations, and individuals and organizations doing business with subscribers who have received their certificates from a CA issuing certificates to the public. Relying parties may or may not also be subscribers within a given PKI.

Relying parties must:

1. Read the procedures published in this document;
2. Use the certificates for the permitted uses only;
3. Not assume any authorization attributes are based solely on an entity's possession of a DOEGrids certificate;
4. Notify DOEGrids PKI of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of the incident.

Relying parties may:

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

RFC 2527: §1.3.3

IGTF Classic: §1 (general)

DOEGrids v2.10: §2.1.3.

1.3.5. Other Participants

Such as certificate manufacturing authorities, providers of repository services, and other entities providing PKI-related services.

DOEGrids PKI will provide access to DOEGrids CA information, as outlined in Section 2, on its Web site. The following pages deal with individual items from Section 2:

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>

RFC 2527: N/A

IGTF Classic: §1 (general)

DOEGrids v2.10: §2.1.4.

1.4. Certificate Usage

This subcomponent contains:

- A list of the types of applications for which the issued certificates are suitable, such as electronic mail, retail transactions, contracts, and travel orders, and/or
- A list of the types of applications for which use of the issued certificates is prohibited.

In the case of a CP or CPS describing different levels of assurance, this subcomponent can describe applications or types of applications that are appropriate or inappropriate for the different levels of assurance.

See Section 1.6 .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 DOEGrids 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.

RFC 2527: §1.3.4

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.3.4.

1.4.1. Appropriate Certificate Uses

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. While person certificates may be used for other activities, such as e-mail signing and encryption, these are not supported activities.

RFC 2527: §1.3.4

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.3.4

1.4.2. Prohibited Certificate Uses

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

RFC 2527: §1.3.4

IGTF Classic: §1 (general)

DOEGrids v2.10: §1.3.4.

1.5. Policy Administration

This subcomponent includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP or CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person. As an

alternative to naming an actual person, the document may name a title or role, an e-mail alias, and other generalized contact information. In some cases, the organization may state that its contact person, alone or in combination with others, is available to answer questions about the document.

Moreover, when a formal or informal policy authority is responsible for determining whether a CA should be allowed to operate within or interoperate with a PKI, it may wish to approve the CPS of the CA as being suitable for the policy authority's CP. If so, this subcomponent can include the name or title, electronic mail address (or alias), telephone number, fax number, and other generalized information of the entity in charge of making such a determination. Finally, in this case, this subcomponent also includes the procedures by which this determination is made.

1.5.1. Organization Administering the Document

ESnet administers the DOEGrids CPS. The DOEGrids CPS is managed by the DOEGrids Policy Management Authority.

RFC 2527: §1.4.1

IGTF Classic: §1

DOEGrids v2.10: §1.4

1.5.2. Contact Person

The contact person for questions related to this document is the chairman of the PMA:

John Volmer
Argonne National Laboratory
volmer@anl.gov

The 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 e-mail addresses and phone numbers can be used to request information or report problems (security, access or service failures). Security incidents, access problems or other service failures should be reported to ESnet's trouble-reporting service:

ESnet Trouble e-mail: 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)

[RFC 2527: §1.4.2](#)

[DOEGrids: §1.4](#)

1.5.3. Person Determining CPS Suitability for the Policy

[RFC 2527: §1.4.3](#)

1.5.4. CPS Approval Procedures

The DOEGrids CPS is managed by the DOEGrids Policy Management Authority.

The DOEGrids CA and CPS is accredited under the “Classic CA profile” by the EU Grid Policy Management Authority (EUGridPMA) of the International Grid Trust Federation (IGTF).

[RFC 2527: §8.3](#)

1.6. Definitions and Acronyms

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL,” in this document are to be interpreted as described in RFC 2119 [Brader97].

Note that the force of these words is modified by the requirement level of the document in which they are used.

1. **MUST** This word, or the terms “REQUIRED” or “SHALL,” mean that the definition is an absolute requirement of the specification.
2. **MUST NOT** This phrase, or the phrase “SHALL NOT,” mean that the definition is an absolute prohibition of the specification.
3. **SHOULD** This word, or the adjective “RECOMMENDED,” mean that there may exist valid reasons in particular circumstances to ignore a particular item, but that the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT** This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

[This subcomponent contains a list of definitions for defined terms used within the document, as well as a list of acronyms in the document and their meanings.](#)

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 that a certification authority employs in issuing certificates.

Community Registration Manager (CRM)

One or more Registration Managers (RMs) that serve multiple low request rate sites/Virtual Organizations.

Common Name (CN)

The common name of the subject of a certificate (full name, host name, etc.). Equivalent to Distinguished Name/Subject Name for the purposes of this document (see RFC 2986).

Certificate Signing Request (CSR)

The message sent to a Certification Authority that describes the public key and content that need to be signed.

Distinguished Encoding Rules (DER)

A restricted form of BER, one of a set of encoding rules for the ASN.1 syntax used by X.509 certificates (see X.690).

Distinguished Name (DN)

The complete, unique name of an entity, written as an ordered list of X.500/LDAP attribute-value pairs. Equivalent to Common Name/Subject Name for the purposes of this document (see RFC 4514 and RFC 4519).

DOEGrids PKI

Refers to the whole of the PKI, including the electronic services, the CA managers, RAs, and RAs.

DOEGrids PKI Members

Refers to the CA managers and the RA Points of Contact, who comprise a large subset of the PMA.

DOEGrids PKI Service

Refers to the electronic services of the PKI, computers, Web interfaces, e-mail, 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.

Federal Bridge Certification Authority (FBCA)

FBCA signs certificates of root CAs from other US federal agencies and other interested parties; it attempts to map policies between different PKIs in a standard way to promote interoperability.

Hardware Security Module (HSM)

An HSM provides secure storage and operation of cryptographic data, typically the signing key of a CA or other server (see NIST FIPS-140 document).

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/Virtual Organizations (VOs).

Online Certificate Status Protocol (OCSP)

A protocol that enables an application to determine the revocation or validity status of a certificate, without need for the entire CRL (see RFC 2560).

Owner

The human individual or organizational group with 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).

Privacy-Enhanced Mail (PEM)

A “printable encoding” of binary objects (such as BER encoded ASN.1 information) that maps every 6 bits of this data into an array of 64 known printable characters. This formatting is also often called base 64 encoding. The encoding was defined in RFC 1421 as part of Privacy Enhanced Mail (PEM) standards and the standard became associated with the encoding.

Person Certificate

A certificate associated with a unique human being.

Personal Identification Number (PIN)

In the context of a Certification Practice Statement, an example of activation data.

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 who has been chosen to handle all communications about policy matters with the DOEGrids PMA.

Private Registration Manager (RM)

Registration Managers that serve sites/VOs with high certificate request rates, 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”

The Registration 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 (DOEGrids) 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.

Secure Sockets Layer (SSL)

See TLS.

Security Incident

An incident that has the potential of private key loss or compromise, regardless of whether the compromise or loss was definitive. 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.

Subject Name

The person who applied for and was issued a certificate. Equivalent to Distinguished Name for the purposes of this document.

Subscriber

The person who applied for and was issued a certificate.

Transport Layer Security (TLS)

TLS is a protocol that supports communications security over the Internet (see RFC 2246 and 4346).

Virtual Organization (VO)

An organization created to represent a particular research or development effort, independent of the physical sites where the scientists or engineers work.

[RFC 2527: N/A](#)

[IGTF Classic: §1 \(general, use of terms\)](#)

[DOEGrids v2.10: §1.1.1.](#)

1.6.1. Definitions

RFC 2527: N/A

IGTF Classic: §1 (general, use of terms)

1.6.2. Acronyms

RFC 2527: N/A

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

DOEGrids PKI will operate a secure online repository that contains:

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

RFC 2527: §2.1.5, 2.6

IGTF Classic: §6 (general)

DOEGrids v2.10: §2.6.1

2.1. Repositories

An identification of the entity or entities that operate repositories within the PKI, such as a CA, certificate manufacturing authority, or independent repository service provider.

Repository of certificates and CRLs can be found in the service's LDAP directory: LDAP.DOEGrids.org or on its Web site at 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://crl.doegrids.org/1c3f2ca8/1c3f2ca8.r0>

<http://pki1.doegrids.org/CRL/1c3f2ca8.r0>

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 (<http://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 ESnet's CP/CPS.

RFC 2527: §2.6.4

IGTF Classic: §6 (general)

DOEGrids: §2.6.4

2.2. Publication of Certification Information

The responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates, which may include the responsibilities of making the CP or CPS publicly available using various mechanisms and also of identifying components, subcomponents, and elements of such documents that exist but are not made publicly available due to their sensitivity (e.g., security controls, clearance procedures, or trade secret information).

RFC 2527: §2.6.1, 8.2

2.3. Time or Frequency of Publication

When information must be published and the frequency of publication.

- Certificates will be published to the DOEGrids PKI repository as soon as issued.
- CRLs will be published **whenever a revocation occurs**, and the CRL is also refreshed once daily, with nextUpdate set to +30 days.
- All DOEGrids PKI documents will be published to the project Web site as they are updated.

RFC 2527: §2.6.2, 8.2

DOEGrids v2.10: §2.6.2

2.4. Access Controls on Repositories

Access control on published information objects including CPs, CPS, certificates, certificate status, and CRLs.

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

DOEGrids CPS, certificates, CRLs (in general, the content described in §2.1) and some related documents are available on a read-only basis to the general public. Write access to the repositories is managed by DOEGrids operations and ESnet system administrators.

RFC 2527: §2.6.3

DOEGrids v2.10: §2.6.3

3. IDENTIFICATION AND AUTHENTICATION

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. It also describes how parties requesting re-key or revocation are authenticated. This component also addresses naming practices, including the recognition of trademark rights in certain names.

RFC 2527: §3

IGTF Classic: §3 (general)

3.1. Naming

This subcomponent includes the following elements regarding naming and identification of the subscribers.

RFC 2527: §3.1

3.1.1. Types of Names

Types of names assigned to the subject, such as X.500 distinguished names, RFC 822 names, and X.400 names.

X.500 style names are used.

See Section 7.1.3 for more details.

RFC 2527: §3.1.1

DOEGrids v2.10: §3.1.1

3.1.2. Need for Names to be Meaningful

Whether names have to be meaningful or not.

Subscriber CN (common name) components contain a representation of the subscriber's name and a string of digits for disambiguation.

Host or service CN components usually contain a fully qualified domain name (FQDN) of the host to satisfy Grid and TLS security mechanisms. The CN component may also contain other tags associated with the service.

On an experimental basis, DOEGrids CA operations or RAs may permit special service names or additional name forms in the service common name component.

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 five or six random numeric characters (i.e., "John K. Doe 12347") when constructing the Common Name, to assist in establishing uniqueness

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.

See §7.1 for typical examples.

See following sections for additional requirements.

RFC 2527: §3.1.2

DOEGrids v2.10: §3.1.2

IGTF Classic: §3

3.1.3. Anonymity or Pseudonymity of Subscribers

Whether or not subscribers can be anonymous or pseudonymous, and if they can, what names are assigned to or can be used by anonymous subscribers.

Not supported.

RFC 2527: §3.1.2

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting various name forms, such as the X.500 standard and RFC822.

See §3.1.1, and 3.1.2.

RFC 2527: §3.1.3

3.1.5. Uniqueness of Names

Whether names have to be unique.

Any single subject distinguished name (DN) must be linked to one and only one entity.

RFC 2527: §3.1.4

DOEGrids v2.10: §3.1.3

IGTF Classic: §3

3.1.6. Recognition, Authentication, and Role of Trademarks

RFC 2527: §3.1.5, 3.1.6

3.2. Initial Identity Validation

This subcomponent contains the following elements for the identification and authentication procedures for the initial registration for each subject type (CA, RA, subscriber, or other participant).

RFC 2527: §3.1

3.2.1. Method to Prove Possession of Private Key

If and how the subject must prove possession of the companion private key for the public key being registered, for example, a digital signature in the certificate request message.

Obtaining a personal or individual certificate is initiated by a key generation tag or control that 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 at <http://www.openssl.org>, whether for persons or services, have separate key generation, Certificate Signing Request (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.

RFC 2527: §3.1.7

DOEGrids v2.10: §3.1.4

3.2.2. Authentication of Organization Identity

Identification and authentication requirements for organizational identity of subscriber or participant (CA, RA, subscriber, in the case of certificates issued to organizations or devices controlled by an organization or other participant), for example, consulting the database of a service that identifies organizations or inspecting an organization's articles of incorporation.

Registration Authority membership is approved by the DOEGrids PMA.

Membership in the scope of a particular RA is determined by the RA.

RFC 2527: §3.1.8

3.2.3. Authentication of Individual Identity

Identification and authentication requirements for an individual subscriber or a person acting on behalf of an organizational subscriber or participant (CA, RA, in the case of certificates issued to organizations or devices controlled by an organization, the subscriber, or other participant), including:

- a) Type of documentation and/or number of identification credentials required;
- b) How a CA or RA authenticates the identity of the organization or individual based on the documentation or credentials provided;
- c) If the individual must personally present to the authenticating CA or RA;
- d) How an individual as an organizational person is authenticated, such as by reference to duly signed authorization documents or a corporate identification badge.

DOEGrids RAs generally follow the 1SCP "Identity Vetting: Trusted Third Party mediated" (<http://www.eugridpma.org/guidelines/1scp/>).

OID: 1.2.840.113612.5.2.3.2.1.1

The DOEGrids PKI uses an architecture under which 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 Web site: <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 its procedures in its individual RA appendix in this document.

A name once entered in the DOEGrids CA registry is the property of the original requestor, but is managed by the RA. Management of the ownership of host and service names is delegated to the RA. An existing subscriber name must never be assigned to a new individual. In cases where an RA is asked to assign a pre-existing

name to a particular individual subscriber, RAs must determine whether the requesting subscriber is the “registered owner” of the name requested, and document this determination.

RFC 2527: §3.1.9

DOEGrids v2.10: §3.1.5

3.2.4. Non-Verified Subscriber Information

List of subscriber information that is not verified (called “non-verified subscriber information”) during the initial registration.

RFC 2527: N/A

3.2.5. Validation of Authority

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate.

RFC 2527: §3.1.9

3.2.6. Criteria for Interoperation

In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.

RFC 2527: §4.1

3.3. Identification and Authentication for Re-key Requests

This subcomponent addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants).

RFC 2527: §3.2, 3.3

3.3.1. Identification and Authentication for Routine Re-key

Identification and authentication requirements for routine re-key, such as a re-key request that contains the new key and is signed using the current valid key.

DOEGrids provides the “Replacement certificate” interface, which is used by subscribers to replace expiring personal certificates. This interface requires authentication with an acceptable certificate, and enforces re-key.

RFC 2527: §3.2

DOEGrids v2.10: §3.2

3.3.2. Identification and Authentication for Re-key after Revocation

Identification and authentication requirements for re-key after certificate revocation. One example is the use of the same process as the initial identity validation.

In general, re-key after revocation follows the same rules as an initial registration. In addition, if the subscriber requests the continued use of the same name, or other name already recorded in the DOEGrids CA registry, RAs must determine whether the requestor is the “registered owner” of the name requested, and document this determination.

RFC 2527: §3.3

DOEGrids v2.10: §3.3

3.4. Identification and Authentication for Revocation Request

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA, subscriber, and other participant). Examples include a revocation request digitally signed with the private key whose companion public key needs to be revoked, and a digitally signed request by the RA.

See Section 4.9.2 for details on who can request a certificate revocation.

RFC 2527: §3.4

DOEGrids v2.10: §3.4

Page intentionally left blank

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate.

Within each subcomponent, separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

RFC 2527: §4.4.

IGTF Classic: §4 (general)

DOEGrids v2.10 §4

4.1. Certificate Application

This subcomponent is used to address the following requirements regarding subject certificate application: who can submit a certificate application, such as a certificate subject or the RA; and enrollment process used by subjects to submit certificate applications and responsibilities in connection with this process.

An example of this process is where the subject generates the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the CA. A CA or RA may have the responsibility of establishing an enrollment process in order to receive certificate applications. Likewise, certificate applicants may have the responsibility of providing accurate information on their certificate applications.

Procedures are different depending on whether 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 1,024 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 1.3.3.

Person

The individual making the request is authenticated according to procedures followed by the chosen RA and described in the RA Appendix.

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.

RFC 2527: §4.4

IGTF Classic: §4 (general)

DOEGrids v2.10: §4.1

4.1.1. Who Can Submit a Certificate Application

RFC 2527: §4.1

4.1.2. Enrollment Process and Responsibilities

RFC 2527: §4.1, 2.1.3

4.2. Certificate Application Processing

This subcomponent is used to describe the procedure for processing certificate applications. For example, the issuing CA and RA may perform identification and authentication procedures to validate the certificate application. Following such steps, the CA or RA will either approve or reject the certificate application, perhaps upon the application of certain criteria. Finally, this subcomponent sets a time limit during which a CA and/or RA must act on and process a certificate application.

See 4.1.

RFC 2527: §4.1, 4.2

4.2.1. Performing Identification and Authentication Functions

RFC 2527: §4.1, 4.2

4.2.2. Approval or Rejection of Certificate Applications

RFC 2527: §4.1, 4.2

4.2.3. Time to Process Certificate Applications

The CA managers may 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.

RFC 2527: §4.1, 4.2

DOEGrids v2.10: §4.2

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 instructions on how to download it from the DOEGrids' PKI Web server.

RFC 2527: §4.2

DOEGrids v2.10: §4.3

4.3.1. CA Actions during Certificate Issuance

Describes the actions performed by the CA during the issuance of the certificate, for example a procedure whereby the CA validates the RA signature and RA authority and generates a certificate.

RFC 2527: §4.2

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Describes the notification mechanisms, if any, used by the CA to notify the subscriber of the issuance of the certificate; an example is a procedure under which the CA e-mails the certificate to the subscriber or the RA or e-mails information permitting the subscriber to download the certificate from a Web site.

RFC 2527: §4.2, 4.3

4.4. Certificate Acceptance

No stipulation.

RFC 2527: §4.3, 2.1.3
DOEGrids v2.10: §4.4

4.4.1. Conduct Constituting Certificate Acceptance

The conduct of an applicant that will be deemed to constitute acceptance of the certificate. Such conduct may include affirmative steps to indicate acceptance, actions implying acceptance, or a failure to object to the certificate or its content. For instance, acceptance may be deemed to occur if the CA does not receive any notice from the subscriber within a certain time period; a subscriber may send a signed message accepting the certificate; or a subscriber may send a signed message rejecting the certificate where the message includes the reason for rejection and identifies the fields in the certificate that are incorrect or incomplete.

RFC 2527: §4.3

4.4.2. Publication of the Certificate by the CA

Publication of the certificate by the CA. For example, the CA may post the certificate to an X.500 or LDAP repository.

RFC 2527: §4.3, 2.1.5, 2.6.1

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance by the CA to other entities. As an example, the CA may send the certificate to the RA.

RFC 2527: §4.2, 4.3, 2.1.5, 2.6.1

4.5. Key Pair and Certificate Usage

This subcomponent is used to describe the responsibilities relating to the use of keys and certificates.

RFC 2527: §1.3.4, 2.1.3, 2.1.4

4.5.1. Subscriber Private Key and Certificate Usage

Subscriber responsibilities relating to use of the subscriber's private key and certificate. For example, the subscriber may be required to use a private key and certificate only for appropriate

applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field). Use of a private key and certificate are subject to the terms of the subscriber agreement, the use of a private key is permitted only after the subscriber has accepted the corresponding certificate, or the subscriber must discontinue use of the private key following the expiration or revocation of the certificate.

See Subscriber Obligations, §1.3.3.

RFC 2527: §1.3.4, 2.1.3

4.5.2. Relying Party Public Key and Certificate Usage

Relying party responsibilities relating to the use of a subscriber's public key and certificate. For instance, a relying party may be obligated to rely on certificates only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field), successfully perform public key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using one of the required or permitted mechanisms set forth in the CP/CPS (see Section 4.9 below), and assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

RFC 2527: §1.3.4, 2.1.4

4.6. Certificate Renewal

This subcomponent is used to describe the following elements related to certificate renewal. Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate.

In general, DOEGrids CA no longer permits renewal without re-key; except for ESnet RA participants, who are guaranteed to use a hardware token.

RFC 2527: §4.1, 4.2, 4.3, 3.2

4.6.1. Circumstance for Certificate Renewal

Circumstances under which certificate renewal takes place, such as where the certificate life has expired, but the policy permits the same key pair to be reused.

Personal certificates may be replaced anytime, automatically, until one month after expiration (NB: the current CA software does not permit post-expiration replacement any more).

Service certificates are not currently renewable.

RFC 2527: §4.1, 3.2

4.6.2. Who May Request Renewal

Who may request certificate renewal, for instance, the subscriber, RA, or the CA may automatically renew an end-user subscriber certificate.

Only the subscriber or certificate owner may replace/renew a certificate.

RFC 2527: §4.1, 3.2

4.6.3. Processing Certificate Renewal Requests

A CA or RA's procedures to process renewal requests to issue the new certificate, for example, the use of a token, such as a password, to re-authenticate the subscriber, or procedures that are the same as the initial certificate issuance.

RFC 2527: §4.1, 4.2, 3.2

Grid Administrator, Agent, and RA POC role renewals follow the procedures in Appendix A.

Personal certificate renewals are currently done with the "Replacement Certificate" interface (<https://pki1.doegrids.org/ca/CertBasedSingleEnroll.html>), or by agents (RAGs). See also §3.3.2.

4.6.4. Notification of New Certificate Issuance to Subscriber

RFC 2527: §4.2, 4.3, 3.2

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

RFC 2527: §4.3, 2.1.3, 3.2

4.6.6. Publication of the Renewal Certificate by the CA

Certificates are posted to the public LDAP database on issuance.

RFC 2527: §4.3, 2.1.5, 2.6.1, 3.2

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

RFC 2527: §4.2, 4.3, 2.1.5, 2.6.1, 3.2

4.7. Certificate Re-key

This subcomponent is used to describe the following elements related to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

In general, DOEGrids subscribers and host/service managers re-key certificates at each renewal.

RFC 2527: §4.1, 4.2, 4.3, 3.2

4.7.1. Circumstance for Certificate Re-key

Circumstances under which certificate re-key can or must take place, such as after a certificate is revoked for reasons of key compromise or after a certificate has expired and the usage period of the key pair has also expired.

Certificate renewal **MUST** re-key, except in those cases where the RA can guarantee that a suitable hardware token secures the private key.

Revoked end-entity certificates **MUST** be re-keyed in order to be replaced.

RFC 2527: §4.1, 3.2

4.7.2. Who May Request Certification of a New Public Key

Who may request certificate re-key, for example, the subscriber.

A current certificate holder may re-key his own certificate; an agent or RA may require members of a domain to re-key as appropriate.

RFC 2527: §4.1, 3.2

4.7.3. Processing Certificate Re-keying Requests

A CA or RA's procedures to process re-keying requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance.

RFC 2527: §4.1, 4.2, 3.2

4.7.4. Notification of New Certificate Issuance to Subscriber

RFC 2527: §4.2, 4.3, 3.2

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

RFC 2527: §4.3, 2.1.3, 3.2

4.7.6. Publication of the Re-keyed Certificate by the CA

RFC 2527: §4.3, 2.1.5, 2.6.1, 3.2

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

RFC 2527: §4.2, 4.3, 2.1.5, 2.6.1, 3.2

4.8. Certificate Modification

This subcomponent is used to describe the following elements related to the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key.

RFC 2527: §4.4

4.8.1. Circumstances for Certificate Modification

Circumstances under which certificate modification can take place, such as name change, role change, or reorganization resulting in a change in the DN.

RFC 2527: §4.4.1, 2.1.3

4.8.2. Who May Request Certificate Modification

Who may request certificate modification, for instance, subscribers, human resources personnel, or the RA.

RFC 2527: §4.4.2

4.8.3. Processing Certificate Modification Requests

RFC 2527: §4.4.3

4.8.4. Notification of New Certificate Issuance to Subscriber

A CA or RA's procedures to process modification requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance.

RFC 2527: §4.2, 4.3, 4.4.3

4.8.5. Conduct Constituting Acceptance of Modified Certificate

RFC 2527: §4.3, 4.4.3, 2.1.3

4.8.6. Publication of the Modified Certificate by the CA

RFC 2527: §4.2, 4.3, 4.4.3, 2.1.5, 2.6.1

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

RFC 2527: §4.2, 4.3, 4.4.3, 2.1.5, 2.6.1

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Circumstances under which a certificate may be suspended and circumstances under which it must be revoked, for instance, in cases of subscriber employment termination, loss of cryptographic token, or suspected compromise of the private key.

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.

In general, control of revocation of certificates is delegated to the RA or the registered owner of a certificate.

DOEGrids CA operations will revoke certificates whose e-mail address is nonfunctional for 30 days. A best-effort attempt will be made to notify the RA when the first bounce of the e-mail address occurs.

DOEGrids CA operations will follow the direction of the DOEGrids security incident response team (a DOEGrids PMA function) concerning revocations.

DOEGrids CA operations will deal with other emergency situations as needed.

RFC 2527: §4.9

DOEGrids v2.10: §4.2, 4.5.1

4.9.2. Who Can Request Revocation

Who can request the revocation of the participant's certificate, for example, the subscriber, RA, or CA in the case of an end-user subscriber certificate.

CA operational staff has the authority to revoke any certificate issued by DOEGrids.

A request to revoke 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 DOEGrids CA managers and operational staff.
- The DOEGrids Incident response team
- Any other official entity that is a member of the VO or site.
- Any other official entity responsible for DOEGrids CA—ESnet, LBNL, DOE.

The following entities may request revocation of end-entity certificates for any documentable reason:

- The DOEGrids CA managers and operational staff.
- Any other official entity responsible for DOEGrids CA—ESnet, LBNL, DOE.

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

RFC 2527: §4.4.2

DOEGrids v2.10: §4.5.1, 4.5.2

4.9.3. Procedure for Revocation Request

Procedures used for certificate revocation request, such as a digitally signed message from the RA, a digitally signed message from the subscriber, or a phone call from the RA.

Subscribers may authenticate directly to the CA, using a trusted interface, and revoke their own certificates.

In other cases, the entity requesting the revocation must authenticate itself to an appropriate RA, the RAs' agents, or the DOEGrids CA operations. The method and steps used to authenticate the identity must be recorded by the RA or DOEGrids CA operations, and must in general conform to the methods used to identify a person.

The RA that issued the certificate will be notified immediately about the revocation request and will be allowed one business day to resolve any uncertainties about the circumstances causing the revocation request.

In cases where the DOEGrids CA operations, or other responsible entity determine that a revocation grace period will cause damage to relying parties, revocation is permissible without this grace period. But in any event, the issuing RA must be notified.

RFC 2527: §4.4.3, 2.1.3

DOEGrids v2.10: §4.5.3

4.9.4. Revocation Request Grace Period

The grace period available to the subscriber, within which the subscriber must make a revocation request;

See §4.9.3. A grace period or revocation requirement for subscribers is not currently addressed.

RFC 2527: §4.4.4

4.9.5. Time Within Which CA Must Process the Revocation Request

Revocation requests are processed immediately and automatically by the CA. Revocation requests that require RA or DOEGrids CA operations' attention require one business day for verification and completion.

RFC 2527: N/A

4.9.6. Revocation Checking Requirement for Relying Parties

The mechanisms, if any, that a relying party may use or must use in order to check the status of certificates on which they wish to rely;

Relying parties are encouraged to check for CRLs regularly (see §2.1).

RFC 2527: §4.4.10, 4.4.12, 4.4.14, 2.1.4

4.9.7. CRL Issuance Frequency (if applicable)

If a CRL mechanism is used, the issuance frequency;

See §2.3.

RFC 2527: §4.4.9, 4.8.3

DOEGrids v2.10: §4.5.5

4.9.8. Maximum Latency for CRLs (if applicable)

If a CRL mechanism is used, maximum latency between the generation of CRLs and posting of the CRLs to the repository (in other words, the maximum amount of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated);

Approximately 15 minutes.

RFC 2527: §4.4.9

4.9.9. Online Revocation/Status-Checking Availability

Online revocation/status checking availability, for instance, OCSP and a Web site to which status inquiries can be submitted;

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

RFC 2527: §4.4.11, 4.8.3

DOEGrids v2.10: §4.5.6

4.9.10. Online Revocation Checking Requirements

Requirements on relying parties to perform online revocation/status checks;

No stipulation.

RFC 2527: §4.4.12

DOEGrids v2.10: §4.5.7

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

RFC 2527: §4.4.13, 4.4.14, 4.8.3

DOEGrids v2.10: §4.5.8

4.9.12. Special Requirements Re-key Compromise

Any variations of the above stipulations for which suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).

RFC 2527: §4.4.15

4.9.13. Circumstances for Suspension

Circumstances under which a certificate may be suspended.

The DOEGrids PKI does not support certificate suspension.

RFC 2527: §4.4.5, 2.1.3

DOEGrids v2.10: §4.5.4

4.9.14. Who Can Request Suspension

Who can request the suspension of a certificate, for example, the subscriber, human resources personnel, a supervisor of the subscriber, or the RA in the case of an end-user subscriber certificate.

RFC 2527: §4.4.6

4.9.15. Procedure for Suspension Request

Procedures to request certificate suspension, such as a digitally signed message from the subscriber or RA, or a phone call from the RA.

RFC 2527: §4.4.7, 2.1.3

4.9.16. Limits on Suspension Period

How long the suspension may last.

RFC 2527: §4.4.8

4.10. Certificate Status Services

This subcomponent addresses the certificate status-checking services available to the relying parties.

RFC 2527: §4.4.9-4.4.14

4.10.1. Operational Characteristics

The operational characteristics of certificate status-checking services.

RFC 2527: §4.4.9, 4.4.11, 4.4.13

4.10.2. Service Availability

The availability of such services, and any applicable policies on unavailability.

RFC 2527: §4.4.9, 4.4.11, 4.4.13

4.10.3. Optional Features

Any optional features of such services.

RFC 2527: §4.4.9, 4.4.11, 4.4.13

4.11. End of Subscription

This subcomponent addresses procedures used by the subscriber to end subscription to the CA services, including the revocation of certificates at the end of subscription (which may differ, depending on whether the end of subscription was due to the expiration of the certificate or termination of the service).

RFC 2527: N/A

4.12. Key Escrow and Recovery

This subcomponent contains the following elements to identify the policies and practices relating to the escrowing, and/or recovery of private keys where private key escrow services are available (through the CA or other trusted third parties).

Not supported.

RFC 2527: §6.2.3

DOEGrids v2.10: §6.2.2

4.12.1. Key Escrow and Recovery Policy and Practices

Identification of the document containing private key escrow and recovery policies and practices, or a listing of such policies and practices.

RFC 2527: §6.2.3

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Identification of the document containing session key encapsulation and recovery policies and practices or a listing of such policies and practices.

RFC 2527: §6.2.3

Page intentionally left blank

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This component describes nontechnical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

This component can also be used to define nontechnical security controls on repositories, subject CAs, RAs, subscribers, and other participants. The nontechnical security controls for the subject CAs, RAs, subscribers, and other participants could be the same, similar, or very different.

These nontechnical security controls are critical to trusting the certificates, since lack of security may compromise CA operations resulting for example, in the creation of certificates or CRLs with erroneous information or compromising the CA private key.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, the issuing CA, repository, subject CAs, RAs, subscribers, and other participants.

DOEGrids CA operations are managed by ESnet. Please refer to ESnet's NIST SP 800-53 section PE, "Physical and Environmental Protection" for more information. No requirements are made for non-ESnet participants in the DOEGrids PKI, except where noted.

RFC 2527: §4.5, 5

IGTF Classic: §5 (general)

5.1. Physical Controls

In this subcomponent, the physical controls on the facility housing the entity systems are described.

RFC 2527: §5.1

DOEGrids v2.10: §5.1

5.1.1. Site Location and Construction

Site location and construction, such as the construction requirements for high-security zones and the use of locked rooms, cages, safes, and cabinets;

DOEGrids CA components are housed in ESnet facilities such as the ESnet Data Center, or other locations under contract with various partners and service providers.

RFC 2527: §5.1.1

DOEGrids v2.10: §5.1

5.1.2. Physical Access

Physical access, i.e., mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room monitored by guards or security alarms and requiring movement from zone to zone to be accomplished using a token, biometric readers, and/or access control lists.

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 **DOEGrids CA** security officers and system support staff of ESnet. **Access to locations other than the ESnet Data Center have additional requirements. Please see ESnet's NIST SP 800-53 section PE.**

RFC 2527: §5.1.2

DOEGrids v2.10: §5.1

5.1.3 Power and Air Conditioning

RFC 2527: §5.1.3

5.1.4 Water Exposures

RFC 2527: §5.1.4

5.1.5 Fire Prevention and Protection

RFC 2527: §5.1.5

5.1.6 Media Storage

Media storage, for example requiring the storage of backup media in a separate location that is physically secure and protected from fire and water damage.

RFC 2527: §5.1.6

5.1.7 Waste Disposal

RFC 2527: §5.1.7

5.1.8 Off-Site Backup

DOEGrids CA stores material in a number of off-site locations in a secure manner.

RFC 2527: §5.1.8

5.2. Procedural Controls

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role. Examples of trusted roles include system administrators, security officers, and system auditors.

RFC 2527: §5.2

DOEGrids v2.10: §5.2

5.2.1. Trusted Roles

- CA operator
- Security officer (HSM administrator or security officer)
- System administrator

RFC 2527: §5.2.1

5.2.2. Number of Persons Required per Task

For each task identified, the number of individuals required to perform the task (n out m rule) should be stated for each role. Identification and authentication requirements for each role may also be defined.

See ESnet HSM Operations Guide.

RFC 2527: §5.2.2

5.2.3. Identification and Authentication for Each Role

This component also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

RFC 2527: §5.2.3

5.2.4. Roles Requiring Separation of Duties

RFC 2527: §5.2.1, 5.2.2

5.3. Personnel Controls

All access to the servers and applications that comprise the DOEGrids CA is limited to ESnet staff (LBNL employees). Access is limited as appropriate for the role in support of the CA. Please see ESnet's NIST SP 800-53 section PS, "Personnel Security Class."

RFC 2527: §5.3

DOEGrids v2.10: §5.3

5.3.1. Qualifications, Experience, and Clearance Requirements

Qualifications, experience, and clearances that personnel must have as a condition of filling trusted roles or other important roles. Examples include credentials, job experiences, and official government clearances that candidates for these positions must have before being hired.

No stipulation.

RFC 2527: §5.3.1

5.3.2. Background Check Procedures

Background checks and clearance procedures that are required in connection with the hiring of personnel filling trusted roles or perhaps other important roles; such roles may require a check of their criminal records, references, and additional clearances that a participant undertakes after a decision has been made to hire a particular person;

Follows LBNL requirements for employees.

RFC 2527: §5.3.2

5.3.3. Training Requirements

Training requirements and training procedures for each role following the hiring of personnel.

RFC 2527: §5.3.3

5.3.4. Retraining Frequency and Requirements

Any retraining period and retraining procedures for each role after completion of initial training.

LBNL requires periodic (typically yearly) retraining of employees in security practices, environmental safety, and organizational practices.

RFC 2527: §5.3.4

5.3.5. Job Rotation Frequency and Sequence

Frequency and sequence for job rotation among various roles.

RFC 2527: §5.3.5

5.3.6. Sanctions for Unauthorized Actions

Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems for the purpose of imposing accountability on a participant's personnel.

Follows LBNL practice for employees.

RFC 2527: §5.3.6

5.3.7. Independent Contractor Requirements

Controls on personnel that are independent contractors rather than employees of the entity; examples include: bonding requirements on contract personnel; contractual requirements including indemnification for damages due to the actions of the contractor personnel; auditing and monitoring of contractor personnel; and other controls on contracting personnel.

RFC 2527: §5.3.7

5.3.8. Documentation Supplied to Personnel

Documentation to be supplied to personnel during initial training, retraining, or otherwise.

RFC 2527: §5.3.8

5.4. Audit Logging Procedures

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment.

RFC 2527: §4.5

5.4.1. Types of Events Recorded

Types of events recorded, such as certificate lifecycle operations, attempts to access the system, and requests made to the system.

The following events are recorded and archived

- Certification requests;
- Revocation requests;
- Issued certificates;
- Issued CRLs;

- All e-mail correspondence on the PMA mailing list;
- Certification authority events;
- HSM events (limited);
- Access to devices and servers.

RFC 2527: §4.5.1

DOEGrids v2.10: §4.7.1

5.4.2. Frequency of Processing Log

Frequency with which audit logs are processed or archived, for example, weekly, following an alarm or anomalous event, or whenever the audit log is n% full.

RFC 2527: §4.5.2

5.4.3. Retention Period for Audit Log

Period for which audit logs are kept.

Minimum retention period for CA or computer system logs is three years. Some records are kept indefinitely, and some records not under direct ESnet control follow institutional guidelines; please see ESnet's NIST SP 800-53 section AU, "Audit and Accountability."

RFC 2527: §4.5.3

DOEGrids v2.10: §4.7.2

5.4.4. Protection of Audit Log

Who can view audit logs, for example, only the audit administrator. Protection against modification of audit logs, for instance a requirement that no one may modify or delete the audit records or that only an audit administrator may delete an audit file as part of rotating the audit file; and protection against deletion of audit logs.

Most audit logs are controlled by ESnet support staff. Some facilities logs are available by request.

ESnet staff, CA operations, authorized LBNL staff, and authorized auditors may examine audit records on request.

RFC 2527: §4.5.4

5.4.5. Audit Log Backup Procedures

RFC 2527: §4.5.5

5.4.6. Audit Collection System (Internal vs. External)

Whether the audit log accumulation system is internal or external to the entity.

The CA maintains its own audit files.

System logs and monitoring logs are maintained by ESnet, but by separate organizational components.

RFC 2527: §4.5.6

5.4.7. Notification to Event-Causing Subject

Whether the subject who caused an audit event to occur is notified of the audit action.

No (with some exceptions).

RFC 2527: §4.5.7

5.4.8. Vulnerability Assessments

Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.

See Section 8. ESnet and DOEGrids CA are subject to a variety of security assessment programs and audits.

RFC 2527: §4.5.8

5.5. Records Archival

This subcomponent is used to describe general records archival (or records retention) policies.

ESnet and DOEGrids follow LBNL institutional policies on record management and retention. Please see ESnet's NIST SP 800-53 section AU, "Audit and Accountability."

RFC 2527: §4.6

5.5.1. Types of Records Archived

Types of records that are archived, for example, all audit data, certificate application information, and documentation supporting certificate applications.

All CSRs (which constitute certificate applications) are kept indefinitely.

Versions of CP-CPS documents are kept indefinitely.

RA identification and certification records are maintained by the RA.

RFC 2527: §4.6.1

5.5.2. Retention Period for Archive

For ESnet and DOEGrids, NIST 800-53 AU-11 applies.

RFC 2527: §4.6.2

5.5.3. Protection of Archive

Who can view the archive, for example, a requirement that only the audit administrator may view the archive; protection against modification of the archive, such as securely storing the data on a write-once medium; protection against deletion of the archive; protection against the deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media; and protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.

ESnet staff, CA operations, authorized LBNL staff, and authorized auditors may examine records archives on request.

RFC 2527: §4.6.3

5.5.4. Archive Backup Procedures

RFC 2527: §4.6.4

5.5.5. Requirements for Time-Stamping of Records

RFC 2527: §4.6.5

5.5.6. Archive Collection System (Internal or External)

Whether the archive collection system is internal or external.

RFC 2527: §4.6.6

5.5.7. Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information, such as a requirement that two separate copies of the archive data be kept under the control of two persons, and that the two copies be compared in order to ensure that the archive information is accurate.

RFC 2527: §4.6.7

5.6. Key Changeover

This subcomponent describes the procedures to provide a new public key to a CA's users following a re-key by the CA. These procedures may be the same as the procedure for providing the current key. Also, the new key may be certified in a certificate signed using the old key.

See [ESnet CA Update Operations Guide](#).

A new signing key will be signed by the ESnet root CA and published in the appropriate repositories and distribution systems.

RFC 2527: §4.7

DOEGrids v2.10: §4.8

5.7. Compromise and Disaster Recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately.

See [ESnet CA Update Operations Guide](#).

Compromise will be announced to the DOEGrids PMA, accrediting authorities, and security personnel. Since the circumstances of a disaster or key compromise can vary enormously, the precise details of the response to such events will be determined at the time after consultation with the appropriate authorities and experts.

RFC 2527: §4.8

DOEGrids v2.10: §4.9

5.7.1. Incident and Compromise Handling Procedures

Identification or listing of the applicable incident and compromise reporting and handling procedures.

Security incidents are reported to the ESnet Security Officer. Please refer to ESnet's NIST SP 800-53 section IR, "Incident Response."

RFC 2527: §4.8

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

The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is re-established, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subjects are recertified.

Backup copies of CA databases and other information are kept in the event of system failure.

Evaluation and recertification will be conducted on a case-by-case basis in cooperation with the associated RAs.

RFC 2527: §4.8.1

5.7.3. Entity Private Key Compromise Procedures

The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is re-established, how the new entity public key is provided to the users, and how the subjects are recertified.

See ESnet CA Key Operations Guide.

Compromised end-entity keys follow the policy and practices of §4.9.

RFC 2527: §4.8.3

5.7.4. Business Continuity Capabilities After a Disaster

The entity's capabilities to ensure business continuity following a natural or other disaster. Such capabilities may include the availability of a remote hot-site at which operations may be recovered. They may also include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or at a remote site. For example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

Please consult the ESnet Contingency Plan and other associated documentation for a detailed discussion.

RFC 2527: §4.8.4

5.8. CA or RA Termination

This subcomponent describes requirements relating to procedures for termination and termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

RA termination is managed by the DOEGrids PMA.

If the DOEGrids CA terminates its services, ESnet and the DOEGrids PMA will announce this to the community, and take other steps appropriate to the circumstances of the termination.

RFC 2527: §4.8.9

DOEGrids v2.10: §4.10

6. TECHNICAL SECURITY CONTROLS

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually held key shares). This component may also be used to impose constraints on repositories, subject CAs, subscribers, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, subscribers, and other participants.

Many sections of ESnet's NIST SP 800-53 controls address these issues.

RFC 2527: §6, 2.1.3, 2.1.4

IGTF Classic: §4 (general)

6.1. Key Pair Generation and Installation

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

RFC 2527: §6.1

6.1.1. Key Pair Generation

Who generates the entity public, private key pair? Possibilities include the subscriber, RA, or CA. Also, how is the key generation performed? Is the key generation performed by hardware or software?

Each end entity must generate its own key pair. DOEGrids PKI does not generate private keys. Registration authorities that issue hardware tokens to their subscribers, such as the ESnet RA, may generate keys for their subscribers on these tokens.

RFC 2527: §6.1.1, 6.1.7, 6.1.8

DOEGrids v2.10: §6.1.8

6.1.2. Private Key Delivery to Subscriber

How is the private key provided securely to the entity? Possibilities include a situation where the entity has generated it and therefore already has it, handing the entity the private key physically, mailing a token containing the private key securely, or delivering it in an SSL session.

The DOEGrids PKI never has access to the end-entity private key. The private key is under the control of the subscriber, or, in the case of an RA providing hardware tokens, the RA may generate keys and provide them to its subscribers through an auditable process.

RFC 2527: §6.1.2

DOEGrids v2.10: §6.1.2

6.1.3. Public Key Delivery to Certificate Issuer

How is the entity's public key provided securely to the certification authority? Some possibilities are in an online SSL session or in a message signed by the RA.

Entities' public keys may be delivered to the issuing CA in a secure and trustworthy manner (e.g. SSL/TLS). Public keys are delivered to the CA in self-signed CSRs. Agents bind the public keys to entities through the process disclosed in their Registration Authority appendix; this process is independent of the submission protocol.

RFC 2527: §6.1.3

DOEGrids v2.10: §6.1.3

6.1.4. CA Public Key Delivery to Relying Parties

In the case of issuing CAs, how is the CA's public key provided securely to potential relying parties? Possibilities include handing the public key to the relying party securely in person, physically mailing a copy securely to the relying party, or delivering it in a SSL session.

CA signing certificate may be retrieved from the DOEGrids repository (see §2.1) or by contacting ESnet directly.

The CA signing certificate is available through various trusted repositories (TACAR, IGTF) and through various software distribution mechanisms. These are the preferred delivery mechanisms.

RFC 2527: §6.1.4

DOEGrids v2.10: §6.1.4

6.1.5. Key Sizes

What are the key sizes? Examples include a 1024-bit RSA modulus and a 1024-bit DSA large prime.

DOEGrids CA signs RSA public keys of modulus 1024 bits or greater, and recommends 2048 bit modulus.

RFC 2527: §6.1.5

DOEGrids v2.10: §6.1.5

6.1.6. Public Key Parameters Generation and Quality Checking

Who generates the public key parameters, and is the quality of the parameters checked during key generation?

DOEGrids CA signs keys with exponent 65537.

Keys are generated under user control. In some cases, an RA may operate a token service and generate keys on hardware on behalf of its clientele.

RFC 2527: §6.1.6, 6.1.7

DOEGrids v2.10: §6.1.6, 6.1.7

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

For what purposes may the key be used, or for what purposes should usage of the key be restricted? For X.509 certificates, these purposes should map to the key usage flags in X.509 Version 3 certificates.

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

The DOEGrids online CA signing key **signs end-entity** certificates.

RFC 2527: §6.1.9

DOEGrids v2.10: §6.1.9

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic modules need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

See **ESnet HSM Operations Guide**.

The scope of this section will only include CA private keys (signing keys). Subscriber and participants' keys are out of scope. See Section 6.1.2.

6.2.1. Cryptographic Module Standards and Controls

What standards, if any, are required for the cryptographic module used to generate the keys? A cryptographic module can be composed of hardware, software, firmware, or any combination of them. For example, are the keys certified by the infrastructure required to be generated using modules compliant with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module? Are there any other engineering or other controls relating to a cryptographic module, such as the identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests.

DOEGrids CA signing private key is managed by a FIPS-140 **Level 3 certified** 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 backup service. The private key is **enabled inside the HSM device** by a set of **operator** smart cards.

The keys for these smart cards and the 3DES key used to encrypt the signing private key are generated by the FIPS-140 device (key generation is based on a hardware random number generator). **An additional set of smart cards, the administrative card set, controls the HSM configuration and smart card lifecycle**. Several copies of cards have been created and stored in secure locations.

RFC 2527: §6.2.1, 6.8

DOEGrids v2.10: §6.8

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

Is the private key under n out of m multi-person control? If yes, provide n and m (two-person control is a special case of n out of m, where $n = m = 2$)?

The CA software does not support n of m operations. The HSM administrative tokens use n of m operations.

RFC 2527: §6.2.2

DOEGrids v2.10: §6.2.1

6.2.3. Private Key Escrow

Is the private key escrowed? If so, who is the escrow agent, what form is the key escrowed in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?

Not supported.

RFC 2527: §6.2.3

DOEGrids v2.10: §6.2.2

6.2.4. Private Key Backup

Is the private key backed up? If so, who is the backup agent, what form is the key backed up in (examples include plain text, encrypted, split key), and what are the security controls on the backup system?

Encrypted copies of the private key are backed up, and some copies are kept externally.

RFC 2527: §6.2.4

DOEGrids v2.10: §6.2.3

6.2.5. Private Key Archival

Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?

Not supported.

RFC 2527: §6.2.5

DOEGrids v2.10: §6.2.3

6.2.6. Private Key Transfer into or from a Cryptographic Module

Under what circumstances, if any, can a private key be transferred into or from a cryptographic module? Who is permitted to perform such a transfer operation? In what form is the private key during the transfer (i.e., plaintext, encrypted, or split key)?

The private key is never available as plaintext outside the HSM. Inside the HSM, the plaintext private key is only available for cryptographic operations.

The HSM is enabled and the private key transferred to the module through an HSM operation using the operator token.

RFC 2527: §6.2.6

6.2.7. Private Key Storage on Cryptographic Module

How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?

Encrypted until enabled by an operator token.

RFC 2527: §6.2.6

6.2.8. Method of Activating Private Key

Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?

DOEGrids CA operations enable the CA private key, using one of the operator tokens.

The private key is enabled indefinitely, but see §6.2.9.

RFC 2527: §6.2.7

6.2.9. Method of Deactivating Private Key

Who can deactivate the private key and how? Examples of methods of deactivating private keys include logging out, turning the power off, removing the token/key, automatic deactivation, and time expiration.

A DOEGrids CA operator may deactivate the key using an operator card, or the host machine may be rebooted or power-cycled.

RFC 2527: §6.2.8

6.2.10. Method of Destroying Private Key

Who can destroy the private key and how? Examples of methods of destroying private keys include token surrender, token destruction, and overwriting the key.

The private key may be permanently disabled by destroying the administrative tokens of the HSM.

RFC 2527: §6.2.9

6.2.11. Cryptographic Module Rating

Provide the capabilities of the cryptographic module in the following areas: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Capability may be expressed through reference to compliance with a standard such as U.S. FIPS 140-1, associated level, and rating.

FIPS 140-3.

RFC 2527: §6.2.1, 6.8

6.3. Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, subscribers, and other participants.

The DOEGrids CA signing certificate's current validity period is 5 December, 2002, to 25 January, 2013.

RFC 2527: §6.3

DOEGrids v2.10: §6.3

6.3.1. Public Key Archival

Is the public key archived? If so, who is the archival agent, and what are the security controls on the archival system? Also, what software and hardware need to be preserved as part of the archive to permit use of the public key over time? Note: this subcomponent is not limited to requiring or describing the use of digital signatures with archival data, but rather can address integrity controls other than digital signatures when an archive requires tamper-protection. Digital signatures do not provide tamper-protection or protect the integrity of data; they merely verify data integrity. Moreover, the archival period may be greater than the cryptanalysis period for the public key needed to verify any digital signature applied to archival data.

Certificates issued are kept indefinitely in an internal database, and published in an external repository (see §2) while valid.

RFC 2527: §6.3.1

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

What is the operational period of the certificates issued to the subscriber. What are the usage periods, or active lifetimes, for the subscriber's key pair?

DOEGrids Certificates are issued valid for one year (365 days).

DOEGrids permits use of the Replacement Interface for 30 days after certificate expiration (this functionality is currently disabled).

Certificates for software-based subscriber private keys must be re-keyed after expiration.

Certificates for hardware-based subscriber private keys may be renewed after expiration (this capability is currently only available to participants in the ESnet RA).

RFC 2527: §6.3.2

6.4. Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, pass phrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key, and potentially needs to be considered for the issuing CA, subject CAs, RAs, and subscribers. Such consideration potentially needs to address the entire life-cycle of the activation data, from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, subscriber, and other participants), all of the questions listed in 6.1 through 6.3 potentially need to be answered with respect to activation data rather than with respect to keys.

The CA signing key is managed by an HSM (see §6.2.8).

Subscribers are expected to secure their software private keys with a strong pass phrase, and their hardware private keys with a PIN. Host and service private keys are expected to be secured at an appropriate level for the service in question.

RFC 2527: §6.4

DOEGrids v2.10: §6.4

6.4.1. Activation Data Generation and Installation

RFC 2527: §6.4.1

6.4.2. Activation Data Protection

RFC 2527: §6.4.2

6.4.3. Other Aspects of Activation Data

RFC 2527: §6.4.3

6.5. Computer Security Controls

This subcomponent is used to describe computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999. This subcomponent can also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation-related activity undertaken.

DOEGrids CA follows LBNL and ESnet computer security requirements, refer to ESnet's NIST SP 800-53.

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.

RFC 2527: §6.5.1

DOEGrids v2.10: §6.5.1

6.5.2. Computer Security Rating

No stipulation.

RFC 2527: §6.5.2

DOEGrids v2.10: §6.5.2

6.6. Lifecycle Technical Controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of fail-safe design and implementation techniques (e.g., defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

Please see ESnet's "Service Placement Guide." Also, please see ESnet's NIST SP 800-53 section CM, "Configuration Management," especially parts 2 and 6.

RFC 2527: §6.6

DOEGrids v2.10: §6.6

6.6.1. System Development Controls

RFC 2527: §6.6.1

6.6.2. Security Management Controls

RFC 2527: §6.6.2

6.6.3. Lifecycle Security Controls

RFC 2527: §6.6.3

6.7. Network Security Controls

This subcomponent addresses network security-related controls, including firewalls.

The DOEGrids PKI servers are protected by stateful intrusion detection systems. Access control lists are placed on upstream network interfaces that limit access to and from the public Internet. Active monitoring and blocking is done based on best-practice rule sets.

RFC 2527: §6.7

DOEGrids v2.10: §6.7

6.8. Time-Stamping

This subcomponent addresses requirements or practices relating to the use of time stamps on various data. It may also discuss whether or not the time-stamping application must use a trusted time source.

Most logfiles are time stamped and rely on trusted (but not signed) time information.

RFC 2527: N/A

7. CERTIFICATE, CRL, AND OCSP PROFILES

This component is used to specify the certificate format and, if CRLs and/or Online Certificate Status Protocol (OCSP) are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

It is the intention of the DOEGrids CA PMA and CA operators that DOEGrids certificates conform to the current IGTF-approved OGF Grid Certificate Profile.

RFC 2527: §7.1

IGTF Classic: §4 (general)

7.1. Certificate Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280):

RFC 2527: §7.1

7.1.1. Version Number(s)

X.509 v3.

RFC 2527: §7.1.1

DOEGrids v2.10: §7.1.1

7.1.2. Certificate Extensions

DOEGrids CA signing certificate

Attribute	Critical?	Value
Basic Constraints	Critical	Is CA: yes Path Length Constraint: UNLIMITED
Key Usage	Critical	Digital Signature Key CertSign CRL Sign
Extended Key Usage		Omitted
Netscape Certificate Type	No	SSL Client SSL CA Secure e-mail CA ObjectSigning CA
Subject Key Identifier	No	Key Identifier: <160 bit sha1 hash of DOEGrids CA public key> CA:19:1D:12:8E:6E:A4:38:5D:42:D4:31:0E:08:DB:D9:8D:17:0D:5D
Authority Key Identifier	No	Key Identifier: <160 bit sha1 hash of ESnet Root CA public key> BC:5D:4D:48:2F:F8:35:94:59:AB:5C:89:4B:3E:D1:B2:3A:14:01:EA

Certificate Policies		Omitted
CRL Distribution Points		Omitted
Subject Alternative Name	No	RFC822Name: DOEGrids-CA-1@doegrids.org

DOEGrids End Entity certificates

The current default extensions are shown below. Other combinations of extensions may appear if technically feasible and not in conflict with accreditation or security requirements.

Attribute	Critical?	Value
Basic Constraints	Critical	Omitted: ASN.1 compiler removes default empty sequences
Netscape Certificate Type	No	SSL Client Secure e-mail
Netscape Certificate Type (service)	No	SSL Client SSL Server
Key Usage	Critical	Digital Signature Key Encipherment
Key Usage (service)	Critical	Digital Signature Key Encipherment Data Encipherment
Extended Key Usage	No	Omitted
Authority Key Identifier	No	Key Identifier: <160 bit SHA1 hash of DOEGrids CA public key>
Subject Key Identifier	No	Key Identifier: <160 bit SHA1 hash of DOEGrids EE public key>
Certificate Policies	No	Certificate Policies = OID of this CPS (see §1.2) OID of current IGTF Classic Profile OID of current 1SCP Trusted Thirty Party Identity vetting
CRL Distribution Points	No	http://crl.doegrids.org/1c3f2ca8/1c3f2ca8.crl
Subject Alternative	No	RFC822Name = <subject's public e-mail address>

Name		
Subject Alternative Name (service)	No	RFC822Name = <responsible party's public e-mail address> DNSname= <FQDN of host>

RFC 2527: §7.1.2

DOEGrids v2.10: §7.1.2

7.1.3. Algorithm Object Identifiers

Signature SHA1withRSA - 1.2.840.113549.1.1.5

Keying material RSA - 1.2.840.113549.1.1.1

MD5 hash function is not used.

RFC 2527: §7.1.3

DOEGrids v2.10: §7.1.3

7.1.4. Name Forms

OU=Hosts is for internal use of DOEGrids only.

Issuer: CN=DOEGrids 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 string of up to six random numeric characters added for uniqueness. (i.e. "John K. Doe 98765"):

CN= John K. Doe 98765, 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=foo.example.com, 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/foo.example.com, OU=Services, DC= doegrids, DC=org
- CN=FTP/131.243.2.12, OU=Services, DC= doegrids, DC=org
- CN=foo.example.com, OU=Services, DC= doegrids, DC=org

RFC 2527: §7.1.4

DOEGrids v2.10: §7.1.4

7.1.5. Name Constraints

Not supported.

[RFC 2527: §7.1.5](#)

[DOEGrids v2.10: §7.1.5](#)

7.1.6. Certificate Policy Object Identifier

Same as this document. See [§1.2](#).

[RFC 2527: §7.1.6](#)

[DOEGrids v2.10: §7.1.6](#)

7.1.7. Usage of Policy Constraints Extension

Not supported.

[RFC 2527: §7.1.7](#)

[DOEGrids v2.10: §7.1.7](#)

7.1.8. Policy Qualifiers Syntax and Semantics

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

[RFC 2527: §7.1.8](#)

[DOEGrids v2.10: §7.1.8](#)

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Not supported.

[RFC 2527: §7.1.9](#)

7.2. CRL Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280).

[RFC 2527: §7.2](#)

X.509 v2

[RFC 2527: §7.2](#)

[DOEGrids v2.10: §7.2.1](#)

7.2.1. CRL and CRL Entry Extensions

CRL and CRL entry extensions populated and their criticality.

The DOEGrids CRL consists of headers, extensions, and a list of revoked certificates, following the structure of the current PKIX profile.

Expired certificates are removed from the CRL.

DOEGrids CA publishes a global CRL.

CRL header and global extensions:

Certificate Revocation List Header	Value
Version	X.509V2
Signature	SHA1withRSA
Issuer	DOEGrids CA subject name (namely CN=DOEGrids CA 1, OU=Certificate Authorities, DC=DOEGrids, DC=org).
ThisUpdate	Varies; date/time CRL published
NextUpdate	thisUpdate +30 days
X509v3 CRL Number	Sequence number (monotonically increasing) of this CRL

CRL entries:

Revoked certificate entry	Required	Value
Serial number	Yes	Serial number of revoked certificate
Revocation date	Yes	Date/time of revocation
Revocation reason	No	Any of X.509 CRL Reason code
Invalidity date	No	As determined by revocation agent

DOEGrids CA may publish other CRLs using other issuers or sets of partial CRLs (indirect and / or delta CRLs).

RFC 2527: §7.2.1

DOEGrids v2.10 2527: §7.2.2

7.3. Online Certificate Status Protocol (OCSP) Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the IETF RFC 2560 profile).

Experimental support only at this time.

RFC 2527: N/A

7.3.1. Version Number(s)

Version of OCSP that is being used as the basis for establishing an OCSP system.

RFC 2527: N/A

7.3.2. OCSP Extensions

OCSP extensions populated and their criticality.

RFC 2527: N/A

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment; examples include WebTrust for CAs and SAS 70.

The DOEGrids CA operation may be reviewed by any cross-certifying organization or potential relying organization if approved by the PMA.

DOEGrids CA operations is audited as part of the Lawrence Berkeley National Laboratory's FIPS-199 NIST 800-53 compliance audits on a schedule prescribed by the U.S. Department of Energy. In, addition, DOEGrids CA operations is a component of security and program "peer reviews" of ESnet, on a multi-year periodic basis. DOEGrids CA and PKI are also audited by community members according to the IGTF-approved auditing standards, on a multi-year periodic basis.

RFC 2527: §4.8

IGTF Classic: §7 (general)

DOEGrids v2.10 §2.7

8.1. Frequency or Circumstances of Assessment

Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a CP or CPS, or the circumstances that will trigger an assessment; possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to be operational, or investigation following a possible or actual compromise of security.

RFC 2527: §2.7.1

8.2. Identity/Qualifications of Assessor

The identity and/or qualifications of the personnel performing the audit or other assessment.

RFC 2527: §2.7.2

8.3. Assessor's Relationship to Assessed Entity

The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.

RFC 2527: §2.7.3

8.4. Topics Covered by Assessment

RFC 2527: §2.7.4

8.5. Actions Taken as a Result of Deficiency

Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, revocation of certificates issued to the assessed entity, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.

RFC 2527: §2.7.5

8.6. Communication of Results

Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.

ESnet and DOEGrids PMA control the release of audits and assessments.

[RFC 2527: §2.7.6](#)

9. OTHER BUSINESS AND LEGAL MATTERS

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements, and relying party agreements. This ordering is intended to help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract; instead, it is configured so that its terms and conditions are applied to the parties by separate documents, which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain limitation of liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability.

RFC 2527: §4.2.5

IGTF Classic: §8 (general)

9.1. Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs.

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

RFC 2527: §2.5

DOEGrids v2.10 §2.5

9.1.1. Certificate Issuance or Renewal Fees

RFC 2527: §2.5.1

9.1.2. Certificate Access Fees

RFC 2527: §2.5.2

9.1.3. Revocation or Status Information Access Fees

RFC 2527: §2.5.3

9.1.4. Fees for Other Services

Fees for other services, such as providing access to the relevant CP or CPS.

RFC 2527: §2.5.4

9.1.5. Refund Policy

RFC 2527: §2.5.5

9.2. Financial Responsibility

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations.

No financial responsibility is accepted.

RFC 2527: §2.3

DOEGrids v2.10 §2.3

9.2.1. Insurance Coverage

A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants.

RFC 2527: §2.3

9.2.2. Other Assets

A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI, where examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, and a right under an agreement to an indemnity under certain circumstances.

RFC 2527: §2.3

9.2.3. Insurance or Warranty Coverage for End Entities

A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

RFC 2527: §2.3

9.3. Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement.

DOEGrids 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.

DOEGrids PKI does not collect any kind of confidential information.

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

RFC 2527: §2.8

IGTF Classic: §8

DOEGrids v2.10: §2.8

9.3.1. Scope of Confidential Information

The scope of what is considered confidential information.

RFC 2527: §2.8.1, 2.8.3

9.3.2. Information Not Within the Scope of Confidential Information

The types of information that are considered to be outside the scope of confidential information.

RFC 2527: §2.8.2, 2.8.3

9.3.3. Responsibility to Protect Confidential Information

The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

RFC 2527: §2.8, 2.8.3–2.8.7

9.4. Privacy of Personal Information

This subcomponent relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to provide for personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this subcomponent addresses the following, to the extent pertinent under applicable law.

DOEGrids CA follows institutional requirements, namely the LBNL Privacy Policy: <http://www.lbl.gov/Disclaimers.html>.

In particular, certain types of Personally Identifiable Information are not approved for use in DOEGrids CA itself and are not requested or collected by the DOEGrids CA service.

DOEGrids CA collects name, contact information, and affiliation information needed for the purpose of establishing and maintaining eligibility for certification. Users of the DOEGrids CA service should have no expectation of privacy for this information.

DOEGrids RAs may have other rules and other requirements, which should be dealt with in the RA's disclosure.

[RFC 2527: §2.8](#)

9.4.1. Privacy Plan

The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy.

[RFC 2527: N/A](#)

9.4.2. Information Treated as Private

Information that is considered private within the PKI.

[RFC 2527: §2.8.1, 2.8.3](#)

9.4.3. Information not Deemed Private

Information that is not considered private within the PKI.

[RFC 2527: §2.8.2, 2.8.3](#)

9.4.4. Responsibility to Protect Private Information

Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties.

[RFC 2527: §2.8, 2.8.1, 2.8.3](#)

9.4.5. Notice and Consent to Use Private Information

Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information.

[RFC 2527: N/A](#)

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

[RFC 2527: §2.8.4, 2.8.5](#)

9.4.7. Other Information Disclosure Circumstances

RFC 2527: §2.8.6, 2.8.7

9.5. Intellectual Property Rights

This subcomponent addresses the intellectual property rights, such as copyright, patent, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

Consistent with the accreditation requirement of IGTF, ESnet/LBNL grants to the IGTF and its member PMAs the right of unlimited redistribution of the documents and metadata required to fulfill the IGTF's mission, namely this CPS document, the signed copies of signing certificates, and contact information (also contained in this document).

In addition, ESnet and DOEGrids CA operations follow institutional requirements concerning copyright, namely <http://www.lbl.gov/Disclaimers.html>, which allows the grant described above.

This CPS document quotes extensively from RFC 3647 for the purpose of guiding editors and readers. It is heavily influenced by and modeled on the BrGrid CPS. Parts of this document are inspired by [INFN CP], [GridCP], [EuroPKI], [TrustID], [NCSA], [PAG], and [FBCA]. Also see Acknowledgments.

RFC 2527: §2.9

DOEGrids v2.10: §2.9

9.6. Representations and Warranties

This subcomponent can include representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate. Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all CAs utilize a subscriber agreement, and that a subscriber agreement must contain a warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

RFC 2527: §2.2

9.6.1. CA Representations and Warranties

RFC 2527: §2.2.1

9.6.2. RA Representations and Warranties

RFC 2527: §2.2.2

9.6.3. Subscriber Representations and Warranties

[RFC 2527: §2.1.3](#)

9.6.4. Relying Party Representations and Warranties

[RFC 2527: §2.1.4](#)

9.6.5. Representations and Warranties of Other Participants

[RFC 2527: N/A](#)

9.7. Disclaimers of Warranties

This subcomponent can include disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

[RFC 2527: §2.2, 2.3.2](#)

9.8. Limitations of Liability

This subcomponent can include limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories: limitations on the elements of damages recoverable and limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery of one party or the other to an amount certain or to an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

DOEGrids 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.

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

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

[RFC 2527: §2.2](#)

[DOEGrids v2.10: §2.2](#)

9.9. Indemnities

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for

losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits.

RFC 2527: §2.1.3, 2.1.4, 2.2, 2.3.1

9.10. Term and Termination

This subcomponent can include the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated. In addition or alternatively, the CP or CPS may include requirements that certain term and termination clauses appear in agreements, such as subscriber or relying party agreements.

RFC 2527: N/A

9.10.1. Term

The term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier.

RFC 2527: N/A

9.10.2. Termination

Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.

RFC 2527: N/A

9.10.3. Effect of Termination and Survival

Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and remain in force. Examples include acknowledgments of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

RFC 2527: N/A

9.11. Individual Notices and Communications with Participants

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective. For example, an RA may wish to inform the CA that it wishes to terminate its agreement with the CA. This subcomponent is different from publication and repository functions, because unlike individual communications described in this subcomponent, publication and posting to a repository are for the purpose of communicating to a wide audience of recipients, such as all relying parties. This subcomponent may establish mechanisms for communication and indicate the contact information to be used to route such communications, such as digitally signed e-mail notices, to a specified address, followed by a signed e-mail acknowledgment of receipt.

RA practices are governed by Appendix A, and the DOEGrids PMA and its charter.

9.12. Amendments

It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change in the CP OID or the CPS pointer (URL). On the other hand, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).

DOEGrids CPS is managed by the DOEGrids PMA.

The DOEGrids PMA will revise this Certificate Policy and Certificate Practices statement as the need arises. Changes are discussed by the Policy Management Authority, taking into account:

- the needs of the user community,
- the impact on the user community,
- the requirements of the accrediting authorities, and
- the latest developments in the authentication theater.

Upon approval by the DOEGrids PMA, changes are announced to subscribers, relying parties, accrediting authorities, and other interested parties.

The DOEGrids CA will make reasonable efforts to remain current with accrediting authorities' changes in requirements or interpretations, audit results, and changes in local requirements or rules. DOEGrids CA operations and members of the DOEGrids PMA will typically maintain contact with these authorities, and offer changes to procedures and documents for approval by the DOEGrids PMA.

DOEGrids PMA reserves the right to make reasonable changes to the operation of the CA and the PKI in advance of the publication of these changes in this document. Operational needs and external requirements may dictate that the PMA act quickly and make changes to the operation of DOEGrids CA. Every effort will be made to announce such changes and to update this document as quickly as possible.

Additionally, from time to time, Lawrence Berkeley National Laboratory and ESnet may be required to modify the operation of DOEGrids CA. LBNL and ESnet are the legal entities responsible for the equipment, data, and operations of DOEGrids CA and accordingly must prudently respond to external and internal requirements. LBNL and ESnet will make every reasonable effort to:

- provide DOEGrids community and other interested parties with advance warning of impending requirements and actions, and
- cooperate with the PMA in responding to new requirements and addressing user needs.

9.12.1. Procedure for Amendment

The procedures by which the CP or CPS and/or other documents must, may be, or are amended.

Updates may be required by changes in membership, membership needs, changes in IGTF requirements, audits, or other processes. DOEGrids PMA update procedures typically require editing, discussion in the PMA, and a vote (or consensus approval), as described in the DOEGrids PMA charter.

Errors and issues for consideration should be brought to the attention of a DOEGrids PMA member and the DOEGrids PMA Chair (see §1.5.2).

RFC 2527: §8.1

9.12.2. Notification Mechanism and Period

In the case of CP or CPS amendments, change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties, such as subscribers and relying parties, a comment period, a mechanism by which comments are received, reviewed and incorporated into the document, and a mechanism by which amendments become final and effective.

Notifications of changes in policy and practice are made to the DOEGrids PMA membership and to other associated parties.

Once DOEGrids PMA approves a new CPS, the CPS is provided to the IGTF and to TACAR as required.

RFC 2527: §8.1

9.12.3. Circumstances Under Which OID Must Be Changed

The circumstances under which amendments to the CP or CPS would require a change in CP OID or CPS pointer (URL).

The DOEGrids CPS OID is changed whenever the CPS document is changed.

RFC 2527: §8.1

9.13. Dispute Resolution Provisions

This subcomponent discusses procedures utilized to resolve disputes arising out of the CP, CPS, and/or agreements. Examples of such procedures include requirements that disputes be resolved in a certain forum or by alternative dispute resolution mechanisms.

RFC 2527: §2.4.3

9.14. Governing Law

This subcomponent sets forth a statement that the law of a certain jurisdiction governs the interpretation and enforcement of the subject CP or CPS or agreements.

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.

RFC 2527: §2.4.1

DOEGrids v2.10: §2.4.1

9.15. Compliance with Applicable Law

This subcomponent relates to stated requirements that participants comply with applicable law, for example, laws relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction. The CP or CPS could purport to impose such requirements or may require that such provisions appear in other agreements.

RFC 2527: §2.4.1

9.16. Miscellaneous Provisions

This subcomponent contains miscellaneous provisions, sometimes called “boilerplate provisions,” in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements.

RFC 2527: §2.4

9.16.1. Entire Agreement

An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the parties and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter.

RFC 2527: §2.4.2

9.16.2. Assignment

An assignment clause, which may act to limit the ability of a party in an agreement, assigning its rights under the agreement to another party (such as the right to receive a stream of payments in the future) or limiting the ability of a party to delegate its obligations under the agreement.

RFC 2527: N/A

9.16.3. Severability

A severability clause, which sets forth the intentions of the parties in the event that a court or other tribunal determines that a clause within an agreement is, for some reason, invalid or unenforceable, and whose purpose is frequently to prevent the unenforceability of one clause from causing the whole agreement to be unenforceable.

RFC 2527: §2.4.2

9.16.4. Enforcement (Attorneys’ Fees and Waiver of Rights)

An enforcement clause, which may state that a party prevailing in any dispute arising out of an agreement is entitled to attorneys’ fees as part of its recovery, or may state that a party’s waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.

RFC 2527: §2.4.3

9.16.5. Force Majeure

A “force majeure” clause, commonly used to excuse the performance of one or more parties to an agreement due to an event outside the reasonable control of the affected party or parties. Typically, the duration of the excused performance is commensurate with the duration of the delay caused by the event. The clause may also provide for the termination of the agreement

under specified circumstances and conditions. Events considered to constitute force majeure may include so-called “acts of God,” wars, terrorism, strikes, natural disasters, failures of suppliers or vendors to perform, or failures of the Internet or other infrastructure. Force majeure clauses should be drafted so as to be consistent with other portions of the framework and applicable service level agreements. For instance, responsibilities and capabilities for business continuity and disaster recovery may place some events within the reasonable control of the parties, such as an obligation to maintain backup electrical power in the face of power outages.

RFC 2527: N/A

9.17. Other Provisions

This subcomponent is a “catchall” location where additional responsibilities and terms can be imposed on PKI participants that do not neatly fit within one of the other components or subcomponents of the framework. CP and CPS writers can place any provision within this subcomponent that is not covered by another subcomponent.

RFC 2527: N/A

10. COMPLIANCE WITH THE CA CLASSIC PROFILE MINIMUM REQUIREMENTS

This section identifies the sections of this CP/CPS document that address the corresponding requirements set out in IGTF's minimum requirements document (currently version 4.1-b3) for traditional X.509 Certification Authorities issuing long-term credentials (the classic profile) [CCA06]. Appropriate extracts of the document are highlighted in blue below.

1. Section 1

(Intentionally left blank.)

2. General Architecture

There should be a single Certification Authority (CA) organization per country, large region or international organization.

Section 1.3

To achieve sustainability, it is expected that the CAs will be operated as a long-term commitment by institutions or organizations rather than being bound to specific projects.

Section 1.1

The CA structure within each region should not follow the conventional hierarchical model, but there should be a single end-entity-issuing CA. A wide network of Registration Authorities (RA) for each CA is preferred.

Sections 1.1, and 4.1.1

The RAs will handle the tasks of validating the identity of the end entities and authenticating their requests, which will then be forwarded to the CA. The CA will handle the actual tasks of issuing CRLs, signing Certificates/CRLS, and revoking Certificates.

Sections 1.3.2, 4.2.1, 9.6.1, and 9.6.2

3. Identity

Any single-subject distinguished name must be linked to one and only one entity.

Sections 1.3.3, and 3.1.5

Over the entire lifetime of the CA, it must not be linked to any other entity.

Sections 1.3.3 and 3.1.5

Certificates must not be shared among end entities.

Section 3.1.5

3.1 Identity Verifying Rules

A PKI CA must define the role of registration authority (RA), and these registration authorities are responsible for the identity verifying of all end entities, such as natural persons and network entities.

Sections 3.2.3 and 4.2.1

In order for an RA to validate the identity of a person, the subject should contact the RA face to face and present photo ID and/or valid official documents showing that the subject is an acceptable end entity as defined in the CP/CPS document of the CA.

Section 3.2.3

In case of host or service certificate requests, the RA should validate the identity of the person in charge of the specific entities, using a secure method. The RA must ensure that the requestor is appropriately authorized by the owner of the FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate.

Sections 3.2.3 and 3.2.5

The RA must validate the association of the certificate-signing request.

Section 3.2.3

The RAs must record and archive all requests and confirmations.

Section 3.2.3

The CA is responsible for the continued archival and auditability of these records.

Section 3.2.3

The RA must communicate with the CA with secure methods that are clearly defined in the CP/CPS (e.g., signed e-mails, voice conversations with a known person, SSL protected private Web pages that are bi-directionally authenticated).

Section 3.2.3

The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.

Sections 3.4, 4.2.1, 4.3.2, and 6.1.3

In all cases, the certificate request submitted for certification must be bound to the act of identity verifying.

Section 3.2.3

3.2 End-Entity Certificate Expiration, Renewal, and Re-keying

For credentials based on software tokens, credentials should only be re-keyed, not renewed.

Sections 4.6.1 and 4.7.1

For those based on hardware tokens, these may be renewed for a period of up to five years (for equivalent RSA key lengths of 2,048 bits) or three years (for equivalent RSA key lengths of 1024 bits).

Section 4.6.1

No credentials can be renewed or re-keyed for more than five years without a form of identity and eligibility verification, and this procedure must be described in the CP/CPS.

Sections 3.3.1, 4.6.1, 4.6.3, and 4.7.3

4. Operational Requirements

The CA computer, where the signing of the certificates will take place, needs to be a dedicated machine, running no other services than those needed for the CA operations.

Sections 4.3.1, 6.5.1, and 6.7

The CA computer must be located in a secure environment where access is controlled, limited to specific trained personnel.

Section 5.1.2

The CA computer may be

- completely off-line: kept disconnected from any kind of networks at all times.
- HSM – hardware security key management

Sections 5.1 and 6.7

The CA key must have a minimum length of 2048 bits.

Section 5.1.2

For CAs that issue end-entity certificates, the lifetime must be no less than two times of the maximum life time of an end-entity certificate and should not be more than 20 years.

Section 6.3.2

The private key of the CA must be protected with a pass phrase of at least 15 elements that is known only by specific personnel of the Certification Authority, except in the case of a Hardware Security Management (HSM), where an equivalent level of security must be maintained.

Sections 6.2.1 and 6.4.1

Copies of the encrypted private key must be kept on offline mediums in secure places where access is controlled.

Section 5.1.6, 6.2.4, and 6.2.7

4.2 Certificate Policy and Certification Practice Statement Identification

Every CA must have a Certificate Policy and Certification Practice Statement (CP/CPS Document) and assign it a globally unique object identifier (OID).

Section 1.2

CP/CPS documents should be structured as defined in RFC 3647.

Section 1

Whenever there is a change in the CP/CPS, the OID of the document must change and the major changes must be announced to the accrediting PMA and approved before signing any certificates under the new CP/CPS.

Sections 1.2, 2.3, and 9.12.3

All the CP/CPS under which valid certificates are issued must be available on the Web.

Section 2.2

4.3 Certificate and CRL Profile

The accredited authority must publish a X.509 certificate as a root of trust.

Sections 2.2 and 4.10.1

The CA certificate must have the extensions `keyUsage` and `basicConstraints` marked as critical.
Section 7.1.2

The authority shall issue X.509 certificates to end entities based on cryptographic data generated by the applicant, or based on cryptographic data that can be held only by the applicant on a secure hardware token.

Sections 6.1.1, 6.1.2, 6.1.7, and 7.1

The EE keys must be at least 1024 bits long. The EE certificates must have a maximum lifetime of 1 year plus 1 month.

Sections 6.1.5 and 6.3.2

The end-entity certificates must be in X.509v3 format and compliant with RFC 3280, unless explicitly stated otherwise. In the certificate extensions:

- a Policy Identifier must be included and must contain an OID and an OID only
- CRL Distribution Points must be included and contain at least one http URL
- `keyUsage` must be included and marked as critical
- `basicConstraints` should be included, and when included, it must be set to 'CA: false' and marked as critical
- if an OCSP responder, operated as a production service by the issuing CA, is available, `AuthorityInfoAccess` must be included and contain at least one URL
- for certificates bound to network entities, a FQDN shall be included as a `dnsName` in the `SubjectAlternativeName`

Sections 6.1.7, 7.1, and 7.1.2

If a `commonName` component is used as part of the subject DN, it should contain an appropriate presentation of the actual name of the end entity.

Section 3.1.2

The CRLs must be compliant with RFC 3280, and are recommended to be version 2.
Section 7.2.1

The message digests of the certificates and CRLs must be generated by a trustworthy mechanism, like SHA1 (in particular, MD5 must not be used).

Section 7.1.3

4.4 Revocation

The CA must publish a CRL.
Section 2.2

The CA must react as soon as possible, but within one working day, to any revocation request received.
Section 4.9.5

After determining its validity, a CRL must be issued immediately.
Section 2.3

For CAs issuing certificates to end entities, the maximum CRL lifetime must be at most 30 days, and the CA must issue a new CRL at least seven days before expiration and immediately after a revocation.

Sections 2.3 and 4.9.7

The CRLs must be published in a repository at least accessible via the World Wide Web, as soon as issued.

Sections 2.2, 4.9.8, and 4.9.9

Revocation requests can be made by end entities, Registration Authorities and the CA.

Sections 3.4 and 4.9.3

These requests must be properly authenticated.

Sections 3.4 and 4.9.3

Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.

Sections 3.4 and 4.9.3

4.5 CA Key Changeover

When the CA's cryptographic data needs to be changed, such a transition shall be managed; from the time of distribution of the new cryptographic data, only the new key will be used for certificate signing purposes. The overlap of the old and new key must be at least the longest time an end-entity certificate can be valid. The older but still valid certificate must be available to verify old signatures—and the secret key to sign CRLs—until all the certificates signed using the associated private key have also expired.

Section 5.6

5. Site Security

The pass phrase of the encrypted private key must be kept also on an offline medium, separated from the encrypted keys and guarded in a safe place where only the authorized personnel of the Certification Authority have access.

Sections 6.2.1, 6.2.4, 6.2.7, and 6.4.2

6. Publication and Repository Responsibilities

Each authority must publish for its subscribers, relying parties and for the benefit of distribution by the PMA and the federation

- a CA root certificate or set of CA root certificates up to a self-signed root;
- a http or https URL of the Privacy-Enhanced Mail (PEM)-formatted CA certificate;
- a http URL of the PEM or Distinguished Encoding Rules (DER)-formatted Certificate Revocation List;
- a http or https URL of the Web page of the CA, for general information;
- the CP and/or CPS documents;
- an official contact e-mail address for inquiries and fault reporting
- a physical or postal contact address

Sections 2.1, 2.2, and 4.10.1

The CA should provide a means to validate the integrity of its root of trust.

Furthermore, the CA shall provide its trust anchor to a trust anchor repository, specified by the accrediting PMA, via the method specified in the policy of the trust anchor repository.

Sections 1.3.5 and 6.1.4

The repository must be run at least on a best-effort basis, with an intended continuous availability.

Sections 2.4 and 4.10.2

The originating authority must grant to the PMA and the Federation—by virtue of its accreditation—the right of unlimited redistribution of this information.

Section 2.2

7. Audits

The CA must record and archive all requests for certificates, along with all the issued certificates, all the requests for revocation, all the issued CRLs and the login/logout/reboot of the issuing machine.

Section 5.4.1

The CA must keep these records for at least three years. These records must be made available to external auditors in the course of their work as auditor.

Sections 5.4.3, 5.4.4, 5.5.2, and 5.5.3

Each CA must accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.

Section 8.3

The CA should perform operational audits of the CA/RA staff at least once per year. A list of CA and RA personnel should be maintained and verified at least once per year.

Section 8.1

8. Privacy and Confidentiality

Accredited CAs must define a privacy and data release policy compliant with the relevant national legislation.

Sections 9.4, 9.4.2, 9.4.3, and 9.4.7

The CA is responsible for recording, at the time of validation, sufficient information regarding the subscribers to identify the subscriber.

Section 3.2.3

The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that CA.

Section 4.9.6

9. Compromise and Disaster Recovery

9.1. Due Diligence for End Entities

The CA should make a reasonable effort to make sure that end entities realize the importance of properly protecting their private data. When using software tokens, users are responsible for protecting their private key with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords.

Sections 4.1.2, 6.4.1, and 9.6.3

End entities must request revocation as soon as possible, but within one working day after detection of loss or compromise of the private key pertaining to the certificate, or if the data in the certificate are no longer valid.

Sections 4.1.2, 4.9.2, and 9.6.3

11. REFERENCES

DOE Office of Science: Personally Identifiable Information (PII) Policy, 7 Aug. 2006

<http://iase.disa.mil/policy-guidance/pii-signed-memo-08182006.pdf>

DOE Privacy Program: DOE Order DOE O 206.1, 16 Jan., 2009

<http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf>

EuroPKI: EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000

FBCA CP: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December, 1999

http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

GridCP: <http://gridcp.es.net/> Global Grid Forum CP

IGTF Classic Profile: Profile for Traditional X.509 Public Key Certification Authorities with Secured Infrastructure, Version 4.0

<http://www.eugridpma.org/guidelines/IGTF-AP-classic-20050930-4-0.html>

INFN CP: <http://security.fi.infn.it/CA/CPS/> INFN CA Policy and CPS.

NCSA: National Computational Science Alliance, Certificate Policy, Version 0.9.1, 30 June, 1999

NIST FIPS 140 document: 1999

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

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. Chokhani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999

RFC 2560: Myers et al., Online Certificate Status Protocol

<http://www.ietf.org/rfc/rfc2560.txt>

RFC 2986: PKCS #10: Certification Request Syntax Specification, Version 1.7, Nystrom and Kaliski

<http://www.ietf.org/rfc/rfc2986.txt>

RFC 3647: S. Chokhani and W. Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003 [replaces RFC 2527]

<http://www.ietf.org/rfc/rfc3647.txt>

RFC 4514: String Representation of Distinguished Names, Zeilinga et al.

<http://www.ietf.org/rfc/rfc4514.txt>

RFC 4519: Schema for User Applications, Zeilinga et al.

<http://www.ietf.org/rfc/rfc4519.txt>

RFC 4519: PKCS #10: Certification Request Syntax Specification, Version 1.7, Nystrom and Kaliski

<http://www.ietf.org/rfc/rfc4519.txt>

PKI Assessment Guide: PKI Assessment Guidelines (PAG)

<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

TrustID: TrustID Certificate Policy

<http://www.digsigtrust.com/certificates/policy/tsindex.html>

[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>

Webtrust for CAs Assessment Guidelines: AICPA/CICA WebTrust Program for Certification Authorities, Version 1.0, August 25, 2000

http://www.webtrust.org/certauth_fin.htm

X.690: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>

12. ACKNOWLEDGMENTS

Version 3.1—Edited by Michael Helm, Victoria Elliott, Dhiva Muruganatham, Doug Olson, Dan Peterson, and John Volmer.

Version 3.0—Edited by Michael Helm and Victoria Elliott. Template developed by Bruce Balfour from BrGrid CPS written by Vinod Rebello.

Version 2.x—Edited and written by Tony Genovese and Michael Helm, with many contributions from Doug Olson and Mary Thompson. Ian Nielsen contributed the RA/agent procedures, based on CERN CA procedures.

Version 1.x —Written and edited by Tony Genovese, with contributions from Michael Helm and many others in the DOE Science Grid; based heavily on INFN CPS, with additional material drawn from the Global Grid Forum CP working group, the 1999 NCSA CP, the Federal Bridge CA documents, the ABA PKI Assessment Guidelines (PAG), EuroPKI CP, and others.

Page intentionally left blank

LIST OF CHANGES

3.1	April, 2009	<p>The following lists the changes for this version:</p> <ol style="list-style-type: none"> 1. §1.1 – Reserve the right to change in advance. 2. §1.2 – OID assignment references. 3. §1.3.3 – Subscribers must now protect private keys with a minimum of TWELVE character passphrase. 4. §1.5.4 – CPS approval procedures 5. §1.5.1/2 – Clarification. 6. Adds definition of PIN. 7. §2.3 – CRL clarification. 8. §2.4 – Access control on repository clarification. 9. §3.1.x – More details about naming, uniqueness. 10. §3.1.5 – Single name, single entity. 11. §3.2.2 – How membership is determined. 12. §3.2.3 – TTP 1SCP; registered owner, recycling of names provisions. 13. §3.3.1 – Routine re-key procedures. 14. §3.3.2 – Authenticating registered owners. 15. §4.5.1 Correct font color. 16. §4.6/4.7 – Renewal/rekey clarification. 17. §4.9.1/4.9.3 – Clarifying some revocation steps and permissions. 18. §4.9.3 – Notifying RA of revocations. 19. §4.9.4 – Grace periods, CRL handling cross-referencing. 20. §4.9.8 – Length of latency. 21. §5 – Management structure, refers to NISTSP 800-53. 22. §5.1.1/2 – Site location. 23. §5.1.8 – Off-site backup. 24. §5.2.1 – Trusted roles. 25. §5.2.1 – No. of persons per task. 26. §5.3.1-5.3.6 – Personnel controls. 27. §5.4.1 – Adds types of events recorded. 28. §5.4.4/5.5.3 – Access to audit records. 29. §5.5.1 – RA & CA records separation (incomplete discussion). 30. §5.7 – Compromise and Disaster Recovery clarifications. 31. §5.7 – RA termination. 32. §6 – HSM and archive clarifications, many changes in general. 33. §6.1.4 – Retrieval of CA cert. 34. §6.1.6 – Use RSA keys only, modulus, and modulus size. 35. §6.3.2 – Lifetime of certs.
-----	-------------	--

		<ul style="list-style-type: none"> 36. §6.4 Activation data. 37. §6.7/6.8 – Remove wrong info, update time stamp. 38. §7 – Many changes, adds tables. 39. §7.1.2 – Began adding CA cert extensions. 40. §7.1.4 – Changed number naming and removed george.lbl.gov from examples. 41. §9.x – Amendments, IP. 42. §9.3 - Delete everything, add site disclaimer, RA disclaimer. 43. §9.4 - Split up disclaimer. 44. §9.5 – Grant of publishing. 45. §9.6 - Pointer to §9.8. 46. §9.7 – Ibid. 47. §9.10.2 – Changeover. 48. §9.10.3 – Effect of change/termination of CPS. 49. Clarify some text in Appendix A.1. 50. Mark Appendix O superseded by ESnet RA. 51. Remove Change Log history before version 3.0.
3.0	March, 2009	<p>The following lists the changes for version 3.0:</p> <ul style="list-style-type: none"> 1. Changes “vetting” to “verifying throughout document. 2. Changes OID, adds table explaining values (section 1.2). 3. Removes cells from table (§1.3.1). 4. Fixes URLs for DOEGrids info (§1.3.3). 5. Changes details on PMA chairman. Appendix M changed to O (CA ops) (§1.5.2). 6. Adds acronyms (§1.6). 7. Fixes out-of-date links (§2.1). 8. Changes CRL frequency (§2.3) 9. Changes alphanumeric to numeric in CN (§3.1.5) 10. Fixes obsolete link (§3.2.3). 11. Subscriber Private Key needs NEW CONTENT (§4.5.1). 12. Text added on hardware tokens (§6.1.1). 13. Private key delivery to subscriber, text added (§6.1.1). 14. Key delivery to cert issuer text added (§6.1.3). 15. Changes DOEGrids’ signing cert validity period to December 2002-January 2013 §6.3). 16. Redescribes compliance audit (§8).

APPENDIX A: GENERAL GUIDELINES FOR DOEGRIDS REGISTRATION AUTHORITIES, AGENTS, AND GRID ADMINISTRATORS

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 officio* members.

[DOEGrids Operations](mailto:DOEGrids-CA-1@DOEGrids.org) (DOEGrids-CA-1@DOEGrids.org) will be responsible for the verification of RA and/or their Agents certificates used to approve/reject/revoke certificates. To ensure that RAs or Agents are aware of their duties, a letter (in the form of an e-mail) acknowledging the RA or agent's role and responsibilities must be sent to [DOEGrids Operations](mailto:DOEGrids-CA-1@DOEGrids.org). Examples of these letters are included in this appendix. DOEGrids Operations require that these letters be digitally signed and mailed to [DOEGrids Operations](mailto:DOEGrids-CA-1@DOEGrids.org). The signed e-mail 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 cannot send digitally signed e-mail, DOEGrids Operations will use another 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

1. Registration Authorities (RA) or their designated Registration Agents (RAGs) will perform all the functions needed to apply certificate issuance policy to potential CA subscribers.
2. 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.
3. Each RA must sign a DOEGrids RA agreement. This Agreement (§ A.3.1) must be sent to DOEGrids Operations as a digitally signed e-mail and resubmitted annually during the renewal of the RA's personal certificate. The certificate used to digitally sign the e-mail to DOEGrids Operations will be used to authorize the RA to approve/revoke certificates.
4. A DOEGrids RA can appoint one or more Registration Agents. These agents do not need the approval of the DOEGrids PMA.
5. Each RA that wishes to appoint an Agent must send a digitally signed e-mail (§ A.3.2) to DOEGrids Operations identifying the person to be an Agent. This e-mail must be resubmitted annually during the renewal process of the Agent's personal certificate.
6. 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 e-mail and resubmitted annually during the renewal of the Agent's personal certificate. The certificate used to digitally sign the e-mail to DOEGrids Operations will be used to authorize the Agent to approve/revoke certificates.

7. 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.
8. The RA or their Agent must check if the requested DN in the certificate request is new and unique. If so, they will continue 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.
9. The RAs and RAg needs to be technically qualified and have the organizational authority to make the decision as to whether the organization will issue a certificate to an applying individual (or to hosts on behalf of an individual who already has a DOEGrids signed certificate).
10. RAs and their Agents, by policy **MAY NOT** do the following:
 11. Sign CA certificates.
 12. Sign a name space not approved by this policy.
 13. 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 Administrators (GridAdmins)

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

The following four e-mail templates are provided for convenience. They are included in the sections that follow.

1. RA Declaration to DOEGrids PMA
This letter must be sent as a signed e-mail 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 e-mail 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 e-mail to the DOEGrids CA operations. It should be sent to: doegrids-ca-1@doegrids.org
4. Letter requesting Grid Administrator Role
This letter is written by the individual requesting to be a Grid Administrator 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 e-mail 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 enrollment 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], [e-mail 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, e-mail 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 e-mail 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 an Agent for [VO/site].
4. I agree only to act on enrollment 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 Administrators

A DOEGrids RA can appoint one or more Grid Administrators to serve their community. These agents do not need the approval of the DOEGrids PMA. The Grid Administrator 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 workload of system administrators who manage large numbers of Grid hosts and services.

These Agents or Grid Administrators 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 Administrator 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 Administrator Role

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

Dear RA of VO/site:

I [*Name of new Grid Administrator*] would like to be a Grid administrator 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 Administrator for [*VO/site*], I have read and understand the responsibilities and tasks assigned to a Grid Administrator as laid out in the DOEGrids CP/CPS.
<http://www.doegrids.org/Docs/CP-CPS.pdf>.
2. I agree that as Grid Administrator 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 PROCEDURES

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 DOEGrids 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 RAs are developed which serve this community.

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 DOEGrids 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 DOEGrids CA.

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

All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail as long as it is verified by secure means before transmission to the DOEGrids CA.

The means of secure communications acceptable are:

- o face-to-face conversation
- o telephone conversation between members of PPDG RA staff
- o telephone conversation between individuals already personally known to each other from face-to-face conversations
- o secure digitally signed e-mail between individuals with certificates from DOEGrids CA.

B.4.3 Steps in Authentication for Certification

B.4.3.1 Person Certificate

A person requests a certificate from the DOEGrids CA community RM.

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

B.4.3.2 Host or Service Certificate

1. A person requests a host or service certificate from the DOEGrids 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 DOEGrids CA 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 request if person has a valid DOEGrids certificate and rejects request if person does not have a valid DOEGrids certificate.

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 DOEGrids 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 DOEGrids 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 DOEGrids CA.

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

All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail 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 NFC RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- secure digitally signed e-mail between individuals with certificates from DOEGrids CA.

C.4.3 Steps in Authentication for Certification

C.4.3.1 Person Certificate

1. A person requests a certificate from DOEGrids 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 e-mail 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 DOEGrids 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 DOEGrids 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.

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 DOEGrids 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 DOEGrids 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 DOEGrids CA guidelines and also pre-existing NERSC authentication and authorization mechanisms.

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

All necessary communications between the DOEGrids 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 DOEGrids CA PMA.

Communication with the NERSC RA on operational issues should be via the e-mail 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 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 e-mail 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 NERSC RA staff.

Telephone conversation between members of NERSC RA staff and NERSC VO users at a 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 e-mail between individuals with certificates from DOEGrids CA.
- Paper documents physically signed and dated by either NERSC RA staff or DOEGrids 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
- E-mail 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 DOEGrids CA, the request includes the name of NERSC VO who will authenticate the request. (secure means)
2. DOEGrids 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 DOEGrids 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 DOEGrids 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.

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 DOEGrids 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 DOEGrids 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 DOEGrids CA. Additional persons may be appointed to the LBNL RA staff by its current members with the approval of the DOEGrids CA.

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

All necessary communications between the DOEGrids 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 DOEGrids 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 DOEGrids activities.

E.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between LBNL 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 e-mail 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 LBNL RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- Secure digitally signed e-mail between individuals with certificates from DOEGrids CA.

E.4.3 Steps in Authentication for Certification

1. A person requests a certificate from DOEGrids CA, the request includes the name of a LBNL RA staff who can authenticate the request. (secure means)
2. DOEGrids CA notifies LBNL RA POC of a certification request. (insecure means)
3. POC retrieves information of certification request from DOEGrids CA (secure means).
4. POC notifies LBNL RA staff member indicated in request that a request is pending including the name, institution and e-mail 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 DOEGrids CA of the authentication of the request (secure means)

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 DOEGrids 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 DOEGrids 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 DOEGrids CA guidelines and existing ORNL authentication and authorization mechanisms. Additional persons may be appointed to the DOEGrids RA staff by ORNL and approved by the DOEGrids CA PMA. ORNL reserves the right to relieve ORNL RA duties from any of its staff members at any time.

F.2.2 Point of Contact (POC) with DOEGrids CA

All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail 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 ORNL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed e-mail between individuals with certificates from DOEGrids 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 e-mails 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 DOEGrids CA. The request includes the requestor's work e-mail 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. DOEGrids CA notifies ORNL RA of a certification request. (insecure means)
 3. ORNL RA staff retrieves information of certificate request from DOEGrids 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 DOEGrids CA.
2. DOEGrids CA notifies ORNL RA of a certification request. (insecure means) .
3. ORNL RA staff retrieves information of certificate request from DOEGrids 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 DOEGrids 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)

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 be 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 e-mail 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 e-mail 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 e-mail 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).

APPENDIX H: PNNL RA OPERATIONAL PROCEDURES

H.1 Background

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

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

All necessary communications between the DOEGrids 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 DOEGrids 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 be 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 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 e-mail 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 PNNL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed e-mail between individuals with certificates from DOEGrids CA
- Paper documents physically signed and dated by either PNNL RA staff or DOEGrids CA staff

H.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 PNNL staff member who will claim the subscriber as a collaborator. (secure means)
2. DOEGrids CA notifies PNNL RA of a certification request including the name, institution and e-mail of the requester. (insecure means)
3. PNNL RA retrieves information of certification request from DOEGrids 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 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 DOEGrids 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 DOEGrids 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 DOEGrids certificates.

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

I.2.2 POC with DOEGrids CA

All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail 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 iVDGL RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversations
- Secure digitally signed e-mail between individuals with certificates from DOEGrids CA.

I.4.3 Steps in authentication for personal certification

1. A person requests a certificate from DOEGrids CA; the request includes the name of an iVDGL RA staff member that can authenticate the request. (Secure means)
2. DOEGrids 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 e-mail 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 DOEGrids 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>)

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 DOEGrids 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 DOEGrids 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 DOEGrids CA.

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

All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail 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 ESG RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- secure digitally signed e-mail between individuals with certificates from DOEGrids CA.

J.4.3 Steps in Authentication for Certification

J.4.3.1 Person Certificate

1. A person requests a certificate from the DOEGrids 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 DOEGrids CA. (secure means)
4. Agent notifies ESG RA staff member indicated in the request that a request is pending including the name, institution and e-mail of the requester. (insecure means)
5. ESG RA staff contacts requester and authenticates request. (secure means)
6. ESG RA staff notifies agent that authentication has occurred. (secure means)
7. Agent notifies DOEGrids 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 DOEGrids 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 DOEGrids CA certificate.
4. Agent approves request if person has a valid DOEGrids certificate and rejects request if person does not have a valid DOEGrids certificate.

APPENDIX K: FNAL RA OPERATIONAL PROCEDURES

K.1 Background

The Fermi National Accelerator Laboratory's (FNAL) DOEGrids 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 DOEGrids. 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 DOEGrids CA guidelines and existing FNAL authentication and authorization mechanisms. Additional persons may be appointed to the DOEGrids RA staff by FNAL.

K.2.2 Point of Contact (POC) with DOEGrids CA

All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail 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 individuals already personally known to each other from face-to-face conversation
- Secure digitally signed communications between individuals with certificates from DOEGrids CA or from the FNAL KCA.
- FNAL-realm Kerberos authenticated requests.
- Paper documents physically signed and dated by either FNAL RA staff or DOEGrids 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 DOEGrids 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. DOEGrids CA notifies FNAL RA of a certification request including the name, institution and e-mail of the requester. (insecure means)
3. FNAL RA retrieves information of certification request from DOEGrids 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).

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 POCs 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

Appendix L: Guidelines for Security Incident Response and Resolution

- 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 DOEGrids CA. Each of these persons will have a valid DOEGrids CA certificate. RAs may appoint Registration Agents (RAGs) at Participating Institutes (see 1.3 below). RAGs will have a valid DOEGrids 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 DOEGrids 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 DOEGrids CA

The LCG Security Group shall identify an individual to be the Point of Contact with DOEGrids CA. All necessary communications between the DOEGrids 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 DOEGrids 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 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 e-mail 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 LCG RA staff
- telephone conversation between individuals already personally known to each other from face-to-face conversations
- secure digitally signed e-mail 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 DOEGrids 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 DOEGrids 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 DOEGrids 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 DOEGrids 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.

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 DOEGrids 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 OSG 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&eMenu=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 DOEGrids CA

All necessary communications between the DOEGrids 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 DOEGrids 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 e-mail 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, e-mail address and telephone number available from a publicly accessible directory of the institution where the subscriber is affiliated.
2. Unsigned e-mail 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 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 e-mail as long as it is verified by secure means before transmission to the DOEGrids CA.

The means of secure communications acceptable are:

- o face-to-face conversation
- o telephone conversation between members of OSG RA staff
- o telephone conversation between individuals already personally known to each other from previous experience
- o secure digitally signed e-mail between individuals with certificates from DOEGrids 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 DOEGrids CA.
2. Agent receives notification of request and takes assignment if appropriate for this RA.
3. Agent checks if person has a valid DOEGrids 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 e-mail 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 e-mail 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 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

This Appendix has been superseded by ESnet RA Operational Procedures, Appendix Q.

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 e-mail 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 e-mail notices for certificate renewals will be referred to the responsible RA.
7. CA operations may revoke certificates when the registered e-mail 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 DOEGrids CA guidelines and also pre-existing Philips Research authentication and authorization mechanisms.

P.2.2 Point of Contact (POC) with DOEGrids CA

All necessary communications between the DOEGrids 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 DOEGrids CA PMA.

Communication with the Philips RA on operational issues should be via the e-mail address al_doegrid_poc@natlab.research.philips.com. This address will forward mail to the Philips Research (US) POC. Alternate e-mail 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 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 e-mail 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.
- 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 e-mail between individuals with certificates from an IGTF Accredited classic CA.
- Paper documents physically signed and dated by either Philips Research (US) RA staff or DOEGrids 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 DOEGrids CA, the request includes the name of Philips Research (US) VO who will authenticate the request. (secure means)
2. DOEGrids 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 DOEGrids 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 DOEGrids 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 0.

APPENDIX Q: ESNET RA OPERATIONAL PROCEDURES

Q.1 Background

The ESnet DOEGrids RA is intended to serve the staff of the Energy Sciences Network. The Network is defined at <http://www.es.net>. This appendix describes how the responsibilities for ESnet RA are implemented.

The Energy Sciences Network is a high-speed network serving thousands of Department of Energy scientists and collaborators worldwide. A pioneer in providing high-bandwidth, reliable connections, ESnet enables researchers at national laboratories, universities and other institutions to communicate with each other using the collaborative capabilities needed to address some of the world's most important scientific challenges.

Managed and operated by the ESnet staff at Lawrence Berkeley National Laboratory, ESnet provides direct connections to all major DOE sites with high-performance speeds, as well as fast interconnections to more than 100 other networks. Funded principally by DOE's Office of Science, ESnet services allow scientists to make effective use of unique DOE research facilities and computing resources, independent of time and geographic location.

ESnet is funded by the DOE Office of Science to provide network and collaboration services in support of the agency's research missions.

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

The proposed use of the certificates includes for two-factor authentication to the network management control plane. Certificates will be stored on tokens and signed by the DOEGrids CA. These certificates will then be used for SSH access to a gateway for management and configuration of ESnet network management plane. The ESnet RA will serve as Registration Authority for CA operations, including the DOEGrids CA, and related services. The ESnet RA will also serve as Registration Authority for staff/service participation in Grids or other projects where X.509 certificates are required. Participating guests of ESnet are also served by this Registration Authority.

The DOEGrids CA is operated by ESnet staff. The operations guidelines are described below in subsection 6.

Q.2 ESnet RA Staff

Q.2.1 Membership

ESnet's staff will serve as the Registration Authority staff in support of ESnet's participation in the DOEGrids. These persons have been designated by ESnet and are ESnet/LBNL employees.

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

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

Q.2.2 Point of Contact (POC) with DOEGrids CA

All necessary communications between the DOEGrids CA and the ESnet RA 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 ESnet. The POC is a defined role of the ESnet Security Officer. The POC shall be a member of the DOEGrids CA PMA.

Q.2.3 Communication with DOEGrids CA

ESnet Registration Authority staff will use DOEGrids-issued certificates for SSL and S/MIME applications.

Q.3 ESnet Community

The ESnet RA will serve the staff and participating guests of ESnet.

Q.4 Authentication Procedures

Q.4.1 Authentication of Individual Identity

Subscribers will be identified by inspection of their LBNL badge. Inspection will take place in person, or via video conference when necessary, by RA staff members.

Q.4.2 Communications

All communications essential for authenticating individual identities and transmitting this information between ESnet RA staff to the DOEGrids CA are carried out in a secure manner. In this context, secure means that 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 e-mail 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, including video conferencing
- Telephone conversation between members of ESnet RA staff
- Telephone conversation between individuals already personally known to each other from face-to-face conversation
- Secure digitally signed e-mail between individuals with certificates from DOEGrids CA
- Paper documents physically signed and dated by either ESnet RA staff or DOEGrids CA staff.

Q.4.3 Steps in Authentication for Certification

1. An individual requests a certificate from DOEGrids CA (secure means).
2. DOEGrids CA notifies ESnet RA of a certification request, including the name, institution and e-mail of the requester (insecure means).

3. ESnet RA retrieves information of the certification request from DOEGrids CA (secure means).

- 3.1. ESnet RA staff verifies the requestor's identity.

If the subscriber is successfully verified, ESnet RA staff approves certificate request (secure means).

Q.5 DOEGrids CA Operations

DOEGrids CA (as well as other CAs and trust services) are operated by ESnet staff. DOEGrids operations require a small number of certificates for staff and services. Occasionally, DOEGrids CA operations staff need to issue certificates to other RA personnel and/or services in order to bootstrap a new organization. To assign, maintain, and document the CA operator role, DOEGrids CA operators and the ESnet RA will follow the DOEGrids procedures for agents.