



UK e-Science Certification Authority
Certificate Policy and Certification Practices
Statement

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

30 October 2003

Contents

- 1 INTRODUCTION 11**
 - 1.1 Overview 11
 - 1.1.1 General definitions 11
 - 1.2 Identification 15
 - 1.3 Community and Applicability 16
 - 1.3.1 Certification authorities 16
 - 1.3.2 Registration authorities 16
 - 1.3.3 End entities (Subscribers) 16
 - 1.3.4 Applicability 16
 - 1.4 Contact Details 17
 - 1.4.1 Specification administration organisation 17
 - 1.4.2 Contact person 17
 - 1.4.3 Person determining CPS suitability for the policy . . . 18

- 2 GENERAL PROVISIONS 19**
 - 2.1 Obligations 19
 - 2.1.1 CA obligations 19
 - 2.1.2 RA obligations 20
 - 2.1.3 Subscriber obligations 21
 - 2.1.4 Relying party obligations 21
 - 2.1.5 Repository obligations 22
 - 2.2 Liability 22
 - 2.2.1 CA liability 22
 - 2.2.2 RA liability 22
 - 2.3 Financial Responsibility 23

2.3.1	Indemnification by relying parties	23
2.3.2	Fiduciary relationships	23
2.3.3	Administrative processes	23
2.4	Interpretation and Enforcement	23
2.4.1	Governing law	23
2.4.2	Severability, survival, merger, notice	23
2.4.3	Dispute resolution procedures	23
2.5	Fees	24
2.5.1	Certificate issuance or renewal fees	24
2.5.2	Certificate access fees	24
2.5.3	Revocation or status information access fees	24
2.5.4	Fees for other services such as policy information	24
2.5.5	Refund policy	24
2.6	Publication and Repositories	24
2.6.1	Publication of CA information	24
2.6.2	Frequency of publication	25
2.6.3	Access controls	25
2.6.4	Repositories	25
2.7	Compliance Audit	25
2.7.1	Frequency of entity compliance audit	25
2.7.2	Identity/qualifications of auditor	26
2.7.3	Auditor's relationship to audited party	26
2.7.4	Topics covered by audit	26
2.7.5	Actions taken as a result of deficiency	26
2.7.6	Communication of results	26
2.8	Confidentiality	26
2.8.1	Types of information to be kept confidential	27
2.8.2	Types of information not considered confidential	27
2.8.3	Disclosure of certificate revocation/suspension information	27
2.8.4	Release to law enforcement officials	27
2.8.5	Release as part of civil discovery	27
2.8.6	Disclosure upon owner's request	27

2.8.7	Other information release circumstances	28
2.9	Intellectual Property Rights	28
3	IDENTIFICATION AND AUTHENTICATION	29
3.1	Initial Registration	29
3.1.1	Types of names	29
3.1.2	Need for names to be meaningful	30
3.1.3	Rules for interpreting various name forms	30
3.1.4	Uniqueness of names	31
3.1.5	Name claim dispute resolution procedure	31
3.1.6	Recognition, authentication and role of trademarks	31
3.1.7	Method to prove possession of private key	31
3.1.8	Authentication of organisation identity	31
3.1.9	Authentication of individual identity	31
3.2	Routine Re-key	32
3.3	Re-key After Revocation	33
3.4	Revocation Request	33
4	OPERATIONAL REQUIREMENTS	35
4.1	Certificate Application	35
4.2	Certificate Issuance	35
4.3	Certificate Acceptance	36
4.4	Certificate Suspension and Revocation	36
4.4.1	Circumstances for revocation	36
4.4.2	Who can request revocation	36
4.4.3	Procedure for revocation request	37
4.4.4	Revocation request grace period	37
4.4.5	Circumstances for suspension	37
4.4.6	Who can request suspension	37
4.4.7	Procedure for suspension request	38
4.4.8	Limits on suspension period	38
4.4.9	CRL issuance frequency	38
4.4.10	CRL checking requirements	38
4.4.11	On-line revocation/status checking availability	38

4.4.12	On-line revocation checking requirements	38
4.4.13	Other forms of revocation advertisements available . . .	38
4.4.14	Checking requirements for other forms of revocation advertisements	38
4.4.15	Special requirements re key compromise	39
4.5	Security Audit Procedures	39
4.5.1	Types of event recorded	39
4.5.2	Frequency of processing log	39
4.5.3	Retention period for audit log	39
4.5.4	Protection of audit log	39
4.5.5	Audit log backup procedures	39
4.5.6	Audit collection system (internal vs external)	40
4.5.7	Notification to event-causing subject	40
4.5.8	Vulnerability assessments	40
4.6	Records Archival	40
4.6.1	Types of event recorded	40
4.6.2	Retention period for archive	41
4.6.3	Protection of archive	41
4.6.4	Archive backup procedures	41
4.6.5	Requirements for time-stamping of records	41
4.6.6	Archive collection system (internal or external)	41
4.6.7	Procedures to obtain and verify archive information . . .	41
4.7	Key Changeover	41
4.8	Compromise and Disaster Recovery	41
4.8.1	Computing resources, software, and/or data are cor- rupted	42
4.8.2	Entity public key is revoked	42
4.8.3	Entity key is compromised	42
4.8.4	Secure facility after a natural or other type of disaster .	42
4.9	CA Termination	42
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECUR- RITY CONTROLS	45
5.1	Physical Controls	45

5.1.1	Site location and construction	45
5.1.2	Physical access	45
5.1.3	Power and air conditioning	45
5.1.4	Water exposures	46
5.1.5	Fire prevention and protection	46
5.1.6	Media storage	46
5.1.7	Waste disposal	46
5.1.8	Off-site backup	46
5.2	Procedural Controls	46
5.2.1	Trusted roles	46
5.2.2	Number of persons required per task	46
5.2.3	Identification and authentication for each role	46
5.3	Personnel Controls	47
5.3.1	Background, qualifications, experience, and clearance requirements	47
5.3.2	Background check procedures	47
5.3.3	Training requirements	48
5.3.4	Retraining frequency and requirements	48
5.3.5	Job rotation frequency and sequence	48
5.3.6	Sanctions for unauthorized actions	48
5.3.7	Contracting personnel requirements	48
5.3.8	Documentation supplied to personnel	48
6	TECHNICAL SECURITY CONTROLS	49
6.1	Key Pair Generation and Installation	49
6.1.1	Key pair generation	49
6.1.2	Private key delivery to entity	49
6.1.3	Public key delivery to certificate issuer	49
6.1.4	CA public key delivery to subscribers	49
6.1.5	Key sizes	50
6.1.6	Public key parameters generation	50
6.1.7	Parameter quality checking	50
6.1.8	Hardware/software key generation	50

6.1.9	Key usage purposes (as per X.509 v3 key usage field)	50
6.2	Private Key Protection	50
6.2.1	Standards for cryptographic module	50
6.2.2	Private key (n out of m) multi-person control	50
6.2.3	Private key escrow	51
6.2.4	Private key backup	51
6.2.5	Private key archival	51
6.2.6	Private key entry into cryptographic module	51
6.2.7	Method of activating private key	51
6.2.8	Method of deactivating private key	51
6.2.9	Method of destroying private key	52
6.3	Other Aspects of Key Pair Management	52
6.3.1	Public key archival	52
6.3.2	Usage periods for the public and private keys	52
6.4	Activation Data	52
6.4.1	Activation data generation and installation	52
6.4.2	Activation data protection	52
6.4.3	Other aspects of activation data	52
6.5	Computer Security Controls	53
6.5.1	Specific computer security technical requirements	53
6.5.2	Computer security rating	53
6.6	Life-Cycle Technical Controls	53
6.6.1	System development controls	53
6.6.2	Security management controls	53
6.6.3	Life cycle security ratings	53
6.7	Network Security Controls	53
6.8	Cryptographic Module Engineering Controls	54
7	CERTIFICATE AND CRL PROFILES	55
7.1	Certificate Profile	55
7.1.1	Version number	55
7.1.2	Certificate extensions	55
7.1.3	Algorithm object identifiers	57

<i>CONTENTS</i>	9
7.1.4 Name forms	57
7.1.5 Name constraints	58
7.1.6 Certificate policy Object Identifier	58
7.1.7 Usage of Policy Constraints extensions	58
7.1.8 Policy qualifier syntax and semantics	58
7.1.9 Processing semantics for the critical certificate policy .	59
7.2 CRL Profile	59
7.2.1 Version number	59
7.2.2 CRL and CRL Entry Extensions	59
8 SPECIFICATION ADMINISTRATION	61
8.1 Specification Change Procedures	61
8.2 Publication and Notification Policies	62
8.3 CPS Approval Procedures	62
A Revision History	63

1 Chapter 1

2 INTRODUCTION

3 This document describes the rules and procedures used by the UK e-Science
4 Certification Authority.

5 1.1 Overview

6 This document is structured according to RFC 2527, [CF99].

7 THIS DOCUMENT IS THE CHANGELOG VERSION BETWEEN
8 VERSIONS 0.9 AND 1.0. IT HAS THE SAME OID AS VERSION 1.0.

9 Apart from minor editorial changes, new items are underlined and deletions
10 are marked with ~~strikeout~~. Linenumbers are not guaranteed to be the same
11 in the two documents.

12 1.1.1 General definitions

13 The document makes use of the following terms:

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 passphrase, or a manually-held key share)
-----------------	--

Authentication	<p>The process of establishing that individuals, organisations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. This process corresponds to the second process involved with identification, as shown in the definition of “identification” below. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organisation, or device. Thus, it is said that a digital signature of a message authenticates the message’s sender.</p>
Certificate Policy (CP)	<p>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.</p>
Certificate Revocation List (CRL)	<p>A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.</p>
Certification Authority (CA)	<p>An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole lifetime.</p>

Certification Practices Statement (CPS)	A statement of the practices, which a certification authority employs in issuing certificates.
CCLRC	Council for the Central Laboratory of the Research Councils. CCLRC is an independent, non-departmental public body of the Office of Science and Technology, part of the Department of Trade and Industry (UK).
<u>GSI</u>	<u>Grid Security Infrastructure. In this document, GSI refers to the Globus GSI as defined in [Gloa] or [Glob].</u>
GridPP Collaboration	UK Particle Physics collaboration funded by PPARC.
Identification	The process of establishing the identity of an individual or organisation, i.e., to show that an individual or organisation is a specific individual or organisation. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organisation corresponds to a real-world identity of an individual or organisation, and (2) establishing that an individual or organisation applying for or seeking access to something under that name is, in fact, the named individual or organisation. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, the issuing CA is the CA that issued the certificate.
Policy Qualifier	Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS.
Registration Authority (RA)	An individual or group of people appointed by an organisation that is responsible for Identification and Authentication of certificate subscribers, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Repository	A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.
Signed Email	In this document, “Signed Email” means an email that satisfies all of the following: (1) it is <i>not encrypted</i> , (2) it has a valid signature, and (3) the certificate corresponding to the private key that generated the signature is a valid e-Science CA certificate, and (4) the Common Name of the certificate bears a reasonable relation to the sender address of the email.
<u>SSL</u>	<u>Secure Sockets Layer. In this document, “SSL” refers to the SSL protocol version 2 or 3, or TLS version 1.0 (RFC2246).</u>

Strong Pass-phrase	In this document, “Strong Pass-phrase” refers to a pass phrase protecting a private key and satisfying the following: it is at least 16 characters long, and contains upper and lower case letters. It is recommended that the pass-phrase contains some non-letter characters in the US-ASCII range (0x20-0x7e) and no letters outside this range.
Subscriber	A person or server to whom a digital certificate is issued.
Validation	The process of identification of certificate applicants. “Validation” is a subset of “Identification” and refers to identification in the context of establishing the identity of certificate applicants.
Virtual Organisation (VO)	An approved programme activity (e.g. pilot project or regional centre).

14 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	1.0
Document date	30 October 2003
Effective from	14 November 2003
Document OID	1.3.6.1.4.1.11439.1.1.1.1.4

15 The document OID is {iso(1) identified-organization(3) dod(6) internet(1)
16 private(4) enterprise(1) cclrc(11439) 1 escience(1) ca(1) cps(1)
17 4}.

18 See also revision history in Appendix A.

19 **1.3 Community and Applicability**

20 **1.3.1 Certification authorities**

21 The e-Science CA self-certifies its own certificate. It does not issue certificates
22 to subordinate CAs.

23 **1.3.2 Registration authorities**

24 A Registration Authority consists of an RA Manager and one or more RA
25 Operators. The RA Manager is appointed within the physical organisation
26 where (s)he is employed, and is in turn responsible for appointing RA Op-
27 erators and to ensure that they operate within the procedure defined by the
28 CPS. The RA Operators are responsible for verifying Subscribers' identities
29 and approving their certificate requests. RA Operators do not issue certifi-
30 cates.

31 **1.3.3 End entities (Subscribers)**

32 The e-Science CA issues certificates for e-Science activities funded by the UK
33 Research Councils. The CA will issue personal, server and service certificates.

34 **1.3.4 Applicability**

35 Certificates issued are of the following types suitable for the following applications:

- 36 • SSL or GSI client (all certificates);
- 37 • SSL or GSI server (server and service certificates only);
- 38 • GSI service (service certificates only);
- 39 • Generating GSI proxies (all certificates);

40 In addition, it is permissible to use certificates for email signing. Using certificates
41 for encryption is not explicitly prohibited but the CA does not support this
42 purpose.

43 Notwithstanding the above, using certificates for purposes contrary to
44 UK law is explicitly prohibited.

- 45 • ~~for server certification and encryption of communications key agreement~~
46 ~~(SSL/TLS);~~
- 47 • ~~Personal authentication;~~
- 48 • ~~Server and service authentication (server and service certificates only).~~
- 49 • ~~for e-mail signing and encryption (S/MIME);~~
- 50 • ~~Object signing.~~

51 **1.4 Contact Details**

52 **1.4.1 Specification administration organisation**

53 The e-Science CA is managed by the UK Grid Support Centre, [GSC].

54 **1.4.2 Contact person**

55 The CA manager (contact person for questions related to this policy docu-
56 ment) is:

57 Dr Jens G Jensen
58 Rutherford Appleton Laboratory
59 Chilton
60 Didcot
61 Oxon
62 OX11 0QX
63 UK
64
65 Phone: +44 1 235 446104
66 Fax: +44 1 235 445945
67 Email: ca-manager@grid-support.ac.uk

68 **1.4.3** Person determining CPS suitability for the pol-
69 **icy**

70 The person mentioned in 1.4.2.

71 Chapter 2

72 GENERAL PROVISIONS

73 2.1 Obligations

74 2.1.1 CA obligations

75 The CA must:

- 76 • publish a CP and a CPS, structured according to RFC2527, [CF99];
- 77 • ensure that services, operations and infrastructure conform to this
78 CP/CPS;
- 79 • issue certificates to entitled subscribers based on validated requests
80 from Registration Authorities;
- 81 • notify the Subscriber of the issuing of the certificate;
- 82 • publish a list of the issued certificates;
- 83 • accept revocation requests according to the procedures outlined in this
84 document;
- 85 • authenticate entities requesting the revocation of a certificate;
- 86 • generate and publish Certificate Revocation Lists (CRL) as described
87 in the CPS;
- 88 • produce a detailed statement of procedure conformant to this CPS and
89 make them available to RA staff.

90 2.1.2 RA obligations

91 The RA Manager must:

- 92 • agree the name of the RA (the values of the OU and L in the DN) with
93 the CA Manager;
- 94 • define the community of Subscribers for which the RA will approve
95 requests, and any requirements in addition to those imposed by this
96 CP/CPS;
- 97 • ensure that (s)he is appointed according to the procedures described in
98 this CP/CPS;
- 99 • appoint one or more RA Operators according to the procedures de-
100 scribed in this CP/CPS;
- 101 • ensure that the Operator(s) operate according to the procedures pro-
102 vided by the CA;
- 103 • in particular, ensure that the RA stores all logs and additional Subscriber
104 information securely, and is released only according to the conditions
105 described in section 2.8;
- 106 • provide access to the logs when requested by the CA.

107 The RA Operator must:

- 108 • adhere to all Subscriber's Obligations (2.1.3)
- 109 • accept certification requests from entitled entities;
- 110 • verify the identity of the Subscriber and keep a log of how each Sub-
111 scription was identified;
- 112 • check that additional location-specific requirements (if any) are fulfilled
113 (an RA may have more stringent requirements for verifying a request
114 than the minimum requirements set out in this policy document - in
115 that case, the RA's web page should list these requirements);
- 116 • provide information to the Subscriber on how to properly maintain a
117 certificate and the corresponding private key;
- 118 • check that the information provided in the certificate request is correct
119 as described in section 3.1.9;

- 120 • sign Subscriber's request when and only when all conditions for issuing
121 a certificate to the Subscriber are fulfilled;
- 122 • Request revocation of a Subscriber's certificate when and only when
123 the RA Operator is aware that (1) the circumstances for revocation
124 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

125 **2.1.3 Subscriber obligations**

126 Subscribers must:

- 127 • read and adhere to the procedures published in this document;
- 128 • generate a key pair using a trustworthy method;
- 129 • use the certificate for the permitted purposes only;
- 130 • authorise the processing and conservation of personal data (as required
131 under the Data Protection Act 1998 [DPA00]);
- 132 • take every precaution to prevent any loss, disclosure or unauthorised
133 access to or use of the private key associated with the certificate, in-
134 cluding:
 - 135 – (personal certificates) selecting a Strong Pass-phrase;
 - 136 – (personal certificates) protecting the pass-phrase from others;
 - 137 – notifying immediately the e-Science CA and any relying parties if
138 the private key is lost or compromised;
 - 139 – requesting revocation if the Subscriber is no longer entitled to a
140 certificate, or if information in the certificate becomes wrong or
141 inaccurate.

142 **2.1.4 Relying party obligations**

143 A Relying Party should accept the Subscriber's certificate for authentication
144 purposes if:

- 145 • the Relying Party is familiar with the CA's CP and the CPS that
146 generated the certificate before drawing any conclusion on trust of the
147 Subscriber's certificate; and

- 148 • the reliance is reasonable and in good faith in light of all circumstances
149 known to the Relying Party at the time of reliance; and
- 150 • the certificate is used for permitted purposes only; and
- 151 • the Relying Party checked the status of the certificate to their own
152 satisfaction prior to reliance.

153 **2.1.5 Repository obligations**

154 The e-Science CA will publish on its web server [CAW] certificates as soon
155 as they are issued, and CRLs according to 4.4.9.

156 **2.2 Liability**

157 **2.2.1 CA liability**

158 The e-Science CA guarantees to issue certificates only to subscribers iden-
159 tified by requests received from RAs via secure routes. The e-Science CA
160 will revoke a certificate only in response to an authenticated request from
161 the Subscriber, or the RA which approved the Subscriber's request, or if
162 it has itself reasonable proof that circumstances for revocation are fulfilled.
163 The e-Science CA does not warrant its procedures, nor takes responsibility
164 for problems arising from its operation or the use made of the certificates
165 it provides and gives no guarantees about the security or suitability of the
166 service.

167 The CA only guarantees to verify Subscriber's identities according to pro-
168 cedures described in this document. In particular, certificates are guaranteed
169 only to reasonably identify the Subscriber (see section 3.1.2).

170 The CA does not accept any liability for financial loss, or loss arising
171 from incidental damage or impairment, resulting from its operation. No
172 other liability, implicit or explicit, is accepted.

173 **2.2.2 RA liability**

174 It is the RA's responsibility to authenticate the identity of subscribers re-
175 questing certificates, according to the practices described in this document.
176 It is the RA's responsibility to request revocation of a certificate if the RA
177 is aware that circumstances for revocation are satisfied.

178 **2.3 Financial Responsibility**

179 No financial responsibility is accepted for certificates issued under this policy.

180 **2.3.1 Indemnification by relying parties**

181 No stipulation.

182 **2.3.2 Fiduciary relationships**

183 No stipulation.

184 **2.3.3 Administrative processes**

185 No stipulation.

186 **2.4 Interpretation and Enforcement**

187 **2.4.1 Governing law**

188 Interpretation of this policy is according to UK Law.

189 **2.4.2 Severability, survival, merger, notice**

190 In the event that the CA ceases operation, all Subscribers, sponsoring organ-
191 isations, RAs, and Relying Parties will be promptly notified of the termina-
192 tion.

193 In addition, all CAs with which cross-certification agreements are current
194 at the time of termination will be promptly informed of the termination.

195 All certificates issued by the CA that reference this Certificate Policy will
196 be revoked no later than the time of termination.

197 **2.4.3 Dispute resolution procedures**

198 No stipulation.

199 **2.5 Fees**

200 **2.5.1 Certificate issuance or renewal fees**

201 No fees are charged for the certification service and therefore there are no
202 financial encumbrances.

203 **2.5.2 Certificate access fees**

204 No fees are charged for certificate access.

205 **2.5.3 Revocation or status information access fees**

206 No fees are charged for access to revocation lists or other certificate status
207 information.

208 **2.5.4 Fees for other services such as policy information**

209 No fees are charged for access to CP and CPS or other CA status informa-
210 tion. The CA reserves the right to charge a fee for the release of personal
211 information, as described in section 2.8.6.

212 **2.5.5 Refund policy**

213 No stipulation.

214 **2.6 Publication and Repositories**

215 **2.6.1 Publication of CA information**

216 The e-Science CA operates an on-line repository [CAW] that contains:

- 217 • The e-Science CA's certificate;
- 218 • Certificates issued;
- 219 • Certificate Revocation Lists;

- 220 • A copy of the most recent version of this CP/CPS and all previous
221 versions since 0.7;
- 222 • Other relevant information.

223 **2.6.2 Frequency of publication**

- 224 • Certificates will be published as soon as they are issued.
- 225 • CRLs will be published as described in 4.4.9.
- 226 • This CP/CPS will be published whenever it is updated.

227 **2.6.3 Access controls**

228 The online repository is maintained on best effort basis and is available sub-
229 stantially on a 24 hours per day, 7 days per week basis, subject to reasonable
230 scheduled maintenance. Outside the period 08:00-17:00 Monday-Friday it
231 may run unattended “at risk”.

232 The e-Science CA does not impose any access control on its CP/CPS, its
233 certificate, issued certificates or CRLs.

234 In the future, the e-Science CA may impose access controls on issued
235 certificates, their status information and CRLs at its discretion. In the event
236 that access controls are implemented, advanced warning of not less than 30
237 days will be given via the CA’s web site.

238 **2.6.4 Repositories**

239 A repository for publishing information detailed in section 2.6.1 is at [CAW].

240 **2.7 Compliance Audit**

241 **2.7.1 Frequency of entity compliance audit**

242 A self-assessment by CCLRC, that the operation is according to this policy,
243 will be carried out at least once a year.

244 In addition, the e-Science CA will accept at least one external Compliance
245 Audit per year when requested by a Relying Party. The entire cost of such
246 an audit must be borne by the requestor.

247 **2.7.2 Identity/qualifications of auditor**

248 No stipulation.

249 **2.7.3 Auditor's relationship to audited party**

250 An external audit can be performed by any UK government department or
251 UK academic institution.

252 **2.7.4 Topics covered by audit**

253 The audit will verify that the services provided by the CA comply with the
254 latest approved version of the CP/CPS.

255 **2.7.5 Actions taken as a result of deficiency**

256 In case of a deficiency, the CA Manager will announce the steps that will be
257 taken to remedy the deficiency. This announcement will include a timetable.

258 **2.7.6 Communication of results**

259 The CA Manager will make the result publicly available on the CA web site
260 with as many details of any deficiency as (s)he considers necessary.

261 **2.8 Confidentiality**

262 The e-Science CA collects a subscriber's name and e-mail address. The
263 subscriber's name as defined in 3.1.2-3, but not e-mail address, is included in
264 the issued personal certificate (server certificates include email address). ~~No~~
265 ~~other subscriber's information is collected.~~ In addition, the RA keeps a copy
266 of the photo id that was used by the Subscriber to verify his/her identity.
267 By making an application for a certificate a Subscriber is deemed to have
268 consented to their personal data being stored and processed, subject to the
269 Data Protection Act 1998.

270 Additionally, for RA Managers and Operators, personal contact informa-
271 tion is kept by the CA (work telephone number, work address).

272 Under no circumstances will the e-Science CA have access to the private
273 keys of any Subscriber to whom it issues a certificate.

274 **2.8.1 Types of information to be kept confidential**

275 The subscriber's e-mail address will be kept confidential (except in the case
276 of server and service certificates when the email address is included in the
277 certificate). The information provided by the Subscriber to verify his/her
278 identity will be kept confidential.

279 **2.8.2 Types of information not considered confidential**

280 Information included in issued certificates and CRLs is not considered con-
281 fidential. RA contact information is not considered confidential since this
282 information is generally available from the web pages of the RA's employer.

283 Statistics regarding certificates issuance and revocation contain no per-
284 sonal information and is not considered confidential.

285 **2.8.3 Disclosure of certificate revocation/suspension in-** 286 **formation**

287 The CA may disclose the time of revocation of a certificate but will not
288 disclose the reason for revocation. The CA may disclose revocation statistics.

289 **2.8.4 Release to law enforcement officials**

290 The CA will not disclose confidential information to any third party unless
291 authorised to do so by the Subscriber or when required by law enforcement
292 officials who exhibit regular warrant.

293 **2.8.5 Release as part of civil discovery**

294 No stipulation.

295 **2.8.6 Disclosure upon owner's request**

296 Disclosure upon owner's request is done according to the Data Protection Act
297 [DPA00], Section 7. Specifically, information is released to the Subscriber
298 if the CA has received a Signed Email from the Subscriber requesting the
299 information. The CA charges no fee for this.

300 The CA ~~may~~will recognise ~~other~~ requests in writing for the release of per-
301 sonal information from a Subscriber provided the Subscriber can be properly
302 authenticated. The CA reserves the right to charge a reasonable fee for the
303 service in this case.

304 **2.8.7 Other information release circumstances**

305 The CA recognises no circumstances for release of personal information other
306 than those described in 2.8.3, 2.8.4, 2.8.5, and 2.8.6.

307 **2.9 Intellectual Property Rights**

308 The e-Science CA does not claim any IPR on certificates which it has issued.

309 Parts of this document are inspired by or copied from (in no particular
310 order) [CFS⁺03], [BG01], [Eur00], [Tru], [NCS99], [FBC99], [Gen01], and
311 [Cec01].

312 Anybody may freely copy from any version of the UK e-Science CA's Cer-
313 tificate Policy and Certification Practices Statement provided they include
314 an acknowledgment of the source.

315 This document typeset with L^AT_EX.

316 Chapter 3

317 IDENTIFICATION AND 318 AUTHENTICATION

319 3.1 Initial Registration

320 3.1.1 Types of names

321 The Subject Name is of the X.500 name type. All parts of the name are
322 encoded as PrintableStrings, except for the Email entry (when applicable)
323 which is encoded as IA5String.

324 The name has one of the following forms:

Person	Name of the Subscriber. The name must include at least one given name in full and the full surname. Rôles are not accepted.
Server	Server fully qualified domain name. The name must be in lower case. IP addresses are not accepted.
Service	As server except the name is prefixed with a service name as defined in 7.1.5.

325
326 Common Names (CNs) must be encoded as PrintableStrings ([WCHK97],[HKYR95]).

327 The maximal length of the CN is 64 characters for all types of certificates.

328 The character set allowed for Common Names in personal certificates is

329 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

330 that is, Space (blank), decimal digits, lower and upper case US ASCII letters,
 331 left and right round brackets, and hyphen. For host and service certificates,
 332 the character '.' (full stop, or period) is also allowed in the Common Name.
 333 For service certificates, the character '/' is also allowed in the Common Name.

334 Email address in server and service certificates must be structured accord-
 335 ing to RFC822. The maximal length of an email address is 128 characters.
 336 Email addresses must be encoded as IA5String but most not contain control
 337 characters or delete.

338 See also 7.1.4.

339 3.1.2 Need for names to be meaningful

340 The Subject Name in a certificate must have a reasonable association with
 341 the authenticated name of the Subscriber. Subscribers must choose a repre-
 342 sentation of their names in the permitted character set (see 3.1.1).

343 The name must not refer to a rôle. Subscribers can neither be anonymous
 344 nor pseudonymous.

345 There is one exception to this rule (other than the root certificate), namely
 346 the certificate with the DN

347 /C=UK/O=eScience/OU=Authority/L=CLRC/CN=ca-operator

348 This certificate is used only within the CA by CA Operators for CA maintenance,
 349 i.e. to allow CA Operators the same access to the public system as RA
 350 Operators. This certificate is also used to sign software deployed by the CA.
 351 This certificate is never used for any other purpose; in particular, it is never
 352 used to access any resources other than the CA's public machine.

353 3.1.3 Rules for interpreting various name forms

354 No stipulation.

3.1.4 Uniqueness of names

The Distinguished Name must be unique for each Subscriber certified by the e-Science CA. If the name presented by the Subscriber is not unique, the CA will ask the Subscriber to resubmit the request with some variation to the common name to ensure uniqueness. In this policy two names are considered identical if they differ only in case or punctuation or whitespace. In other words, case, punctuation and whitespace must not be used to distinguish names. Certificates must apply to unique individuals or resources. Subscribers must not share certificates.

3.1.5 Name claim dispute resolution procedure

No stipulation.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

No stipulation.

3.1.8 Authentication of organisation identity

Only the names of the organisations employing RA staff appear in certificates. Authentication of Organisation Identity is part of the process for appointing an RA. See section 5.3.

3.1.9 Authentication of individual identity

These are the minimum checks mandated by this Policy; individual RAs may impose more stringent checks.

In either case the Subscriber selects which RA is to carry out the identification process.

Person	The Subscriber goes to the selected RA Operator bringing acceptable photo ID.
Server	The requestor must <i>either</i> go to the RA Operator in person and prove his/her identity as for personal certificates, and confirm that (s)he is responsible for the resources mentioned in the request, <i>or</i> send Signed Email to the RA Operator confirming the request and confirming that the requestor is responsible for the resources in question.
Service	As server certificates (the person responsible for a host is regarded as the person responsible for all services running on that host).

380 For personal certificates we allow in exceptional cases an “External” ver-
381 ification for Subscribers who are not able to follow the above procedure for
382 personal certificates: The Subscriber can send an email confirming the re-
383 quest to the CA. The request is accepted by the CA if the email is signed by
384 a certificate from another CA whose certificates are accepted for this purpose
385 by the CA Manager. The list of such CAs will be decided by the CA Manager
386 and is available on the CA’s web site [CAW]. In this case, the CN of the
387 certificate used to sign the email and the CN of the certificate request must
388 be identical. Subscribers should not use this procedure unless there is no al-
389 ternative. Subscribers identified through this procedure will have OU=CLRC,
390 L=External as RA identifier in their certificates.

391 Certificate requests verified by the CA have OU=Authority, L=CLRC as
392 RA identifier.

393 3.2 Routine Re-key

394 No stipulation.

395 **3.3 Re-key After Revocation**

396 There is no re-key after revocation. Subscribers must apply for a new cer-
397 tificate.

398 **3.4 Revocation Request**

399 Anyone can make certificate revocation requests by sending email to the CA.
400 However, the CA will not revoke a certificate unless the request is authenti-
401 cated, or it can be verified independently that there is reason to revoke the
402 certificate. See section 4.4.

403 Authenticated certificate revocation requests may be made by

- 404 • The RA using:
 - 405 – Signed Email to the CA Manager;
 - 406 – Other secure method, as specified in the RA Operator's procedure.
- 407 • The Subscriber by:
 - 408 – Mailing the CA manager directly by Signed Email.

409 Chapter 4

410 OPERATIONAL 411 REQUIREMENTS

412 4.1 Certificate Application

413 Procedures are different if the Subscriber is a person or a server. In every
414 case the Subscriber has to generate his/her own key pair. The minimum
415 key length is 1024 bits. Personal certificates must not be shared; server
416 certificates must be linked to a single network entity. Maximal lifetime of a
417 certificate is one year. The default validity period is one year.

418 Certificate requests are made via the CA's web interface at [CAW].

419 Requests for renewal are made by submitting a request to the CA's web
420 interface via a mutually authenticated SSL connection.

421 4.2 Certificate Issuance

422 The e-Science CA issues the certificate if, and only if, the authentication of
423 the Subscriber is successful. This authentication must be done by an RA or
424 by the CA itself.

425 In the case of renewal, the authentication is considered successful if the
426 DN of the new request matches that of the certificate used by the client when
427 submitting the request. The request needs RA approval to verify that the
428 client is still entitled to a certificate, but the RA need not verify the client's
429 identity.

430 The Subscriber can download the certificate using the CA's web interface.

431 Once a certificate request has been approved by the RA or the CA, the
432 certificate is normally issued by the CA within one working day. The CA
433 adds the new certificate to the published list of certificates issued.

434 If the authentication is unsuccessful, the certificate is not issued and an
435 e-mail with the reason is sent to the Subscriber. In particular, the CA or RA
436 may delete a request if the Subscriber has made no attempt to authenticate
437 him- or herself within 30 days of submitting the request.

438 All issued certificates are issued under the CP/CPS valid at the time of
439 issuance.

440 **4.3 Certificate Acceptance**

441 No stipulation.

442 **4.4 Certificate Suspension and Revocation**

443 **4.4.1 Circumstances for revocation**

444 A certificate will be revoked when the information it contains or the implied
445 assertions it carries are known or suspected to be incorrect or compromised.
446 This includes situations where:

- 447 • The CA is informed that the Subscriber has ceased to be a member of
448 or associated with a UK e-Science program or activity;
- 449 • the Subscriber's private key is lost or suspected to be compromised;
- 450 • the information in the subscriber's certificate is wrong or inaccurate,
451 or suspected to be wrong or inaccurate;
- 452 • the Subscriber violates his/her obligations.

453 **4.4.2 Who can request revocation**

454 A certificate revocation can be requested by:

- 455 • The Registration Authority which authenticated the holder of the cer-
456 tificate;

- 457 • the holder of the certificate;
- 458 • any person presenting proof of knowledge that the subscriber's private
- 459 key has been compromised or that the subscriber's data have changed.

460 **4.4.3 Procedure for revocation request**

461 A revocation request is accepted if:

- 462 • The revocation request is signed with the key corresponding to certifi-
- 463 cate whose revocation is requested; or,
- 464 • The revocation request is signed by the RA who originally approved
- 465 the certificate request.

466 Any other revocation request is accepted only if the entity requesting the
467 revocation is properly authenticated.

468 **4.4.4 Revocation request grace period**

469 If the Subscriber discovers that his/her private key is compromised, (s)he
470 must request revocation:

- 471 • immediately using the online revocation facilities, if (s)he still has ac-
- 472 cess to the private key;
- 473 • otherwise by going to the RA as soon as possible and ask the RA to
- 474 request revocation.

475 The Subscriber should request revocation within one working day if any of
476 the other circumstances for revocation are fulfilled.

477 The revocation will take place within one working day of the CA deter-
478 mining the need for revocation.

479 **4.4.5 Circumstances for suspension**

480 The CA does not offer suspension services.

481 **4.4.6 Who can request suspension**

482 No stipulation.

483 **4.4.7 Procedure for suspension request**

484 No stipulation.

485 **4.4.8 Limits on suspension period**

486 No stipulation.

487 **4.4.9 CRL issuance frequency**

488 CRLs are updated and re-issued within one hour after every certificate revo-
489 cation or at least every week.

490 **4.4.10 CRL checking requirements**

491 No stipulation.

492 **4.4.11 On-line revocation/status checking availability**

493 The latest CRL is always available from the CA web site.

494 **4.4.12 On-line revocation checking requirements**

495 No stipulation.

496 **4.4.13 Other forms of revocation advertisements avail-
497 able**

498 No stipulation.

499 **4.4.14 Checking requirements for other forms of revo-
500 cation advertisements**

501 No stipulation.

502 **4.4.15 Special requirements re key compromise**

503 If the Subscriber's private key is compromised, the Subscriber must ensure
504 that the corresponding certificate is revoked as soon as possible (see 4.4.4),
505 and that all Relying Parties that rely on the certificate in question are in-
506 formed of the compromise.

507 **4.5 Security Audit Procedures**

508 **4.5.1 Types of event recorded**

509 The following events are recorded:

- 510 • certification requests;
- 511 • issued certificates;
- 512 • requests for revocation;
- 513 • issued CRLs;
- 514 • login/logout/reboot of the signing machine.

515 **4.5.2 Frequency of processing log**

516 No stipulation.

517 **4.5.3 Retention period for audit log**

518 The minimum retention period is 3 years.

519 **4.5.4 Protection of audit log**

520 No stipulation.

521 **4.5.5 Audit log backup procedures**

522 No stipulation.

523 **4.5.6 Audit collection system (internal vs external)**

524 No stipulation.

525 **4.5.7 Notification to event-causing subject**

526 No stipulation.

527 **4.5.8 Vulnerability assessments**

528 No stipulation.

529 **4.6 Records Archival**

530 **4.6.1 Types of event recorded**

531 The following events are recorded and archived by the CA:

- 532 • certification requests;
- 533 • issued certificates;
- 534 • requests for revocation;
- 535 • issued CRLs;
- 536 • all e-mail messages received by the CA (not the confirmation messages
537 sent to the Subscribers);
- 538 • all e-mail messages sent by the CA;
- 539 • all documents appointing CA and RA Staff.

540 Each RA must log the following:

- 541 • for each approved request, how it was approved;
- 542 • for each rejected request, why it was rejected;
- 543 • for each approved revocation request, the reason for revocation;
- 544 • for each rejected revocation request, the reason for revocation and the
545 reason the request was rejected.

546 **4.6.2 Retention period for archive**

547 The minimum retention period is 3 years.

548 **4.6.3 Protection of archive**

549 No stipulation.

550 **4.6.4 Archive backup procedures**

551 No stipulation.

552 **4.6.5 Requirements for time-stamping of records**

553 No stipulation.

554 **4.6.6 Archive collection system (internal or external)**

555 No stipulation.

556 **4.6.7 Procedures to obtain and verify archive information**
557

558 No stipulation.

559 **4.7 Key Changeover**

560 The CA will generate a new root key pair one year (the maximal lifetime of
561 a Subscriber's certificate) before the expiry of the CA certificate. In the final
562 year the CA's old certificate will be available for validation purposes only,
563 whereas new certificates and CRLs will be signed with the new CA key.

564 **4.8 Compromise and Disaster Recovery**

565 If the CA's private key is (or is suspected to be) compromised, the CA will:

- 566 • inform the Registration Authorities, Subscribers, Relying Parties, and
567 cross-certifying CAs of which the CA is aware;
- 568 • terminate the certificates and CRL distribution services for certificates
569 and CRLs issued using the compromised key.

570 If an RA Operator's private key is compromised or suspected to be compro-
571 mised, the RA Operator or Manager must inform the CA and request the
572 revocation of the RA Operator's certificate.

573 **4.8.1 Computing resources, software, and/or data are** 574 **corrupted**

575 The CA will take best effort precautions to enable recovery.

576 **4.8.2 Entity public key is revoked**

577 No stipulation.

578 **4.8.3 Entity key is compromised**

579 No stipulation.

580 **4.8.4 Secure facility after a natural or other type of** 581 **disaster**

582 No stipulation.

583 **4.9 CA Termination**

584 Before the e-Science CA terminates its services, it will:

- 585 • inform the Registration Authorities, Subscribers, Relying Parties, and
586 cross-certifying CAs of which the CA is aware;
- 587 • make information of its termination widely available;
- 588 • stop issuing certificates.

589 An advance notice of no less than 60 days will be given in the case of nor-
590 mal (scheduled) termination. The CA Manager at the time of termination
591 shall be responsible for the subsequent archival of all records as required in
592 section 4.6.2.

593 The CA Manager may decide to let the CA issue CRLs only during the
594 last year (i.e. the maximal lifetime of a Subscriber certificate) before the
595 actual termination; this will allow Subscribers' certificates to be used until
596 they expire. In that case notice of termination is given no less than one year
597 and 60 days prior to the actual termination, i.e. no less than 60 days before
598 the CA ceases to issue new certificates.

599 Chapter 5

600 PHYSICAL, PROCEDURAL, 601 AND PERSONNEL 602 SECURITY CONTROLS

603 5.1 Physical Controls

604 5.1.1 Site location and construction

605 No stipulation.

606 5.1.2 Physical access

607 The CA operates in a controlled environment, where access is restricted to
608 authorised people and logged. The signing machine is kept locked in a safe
609 and the private key is locked in a different safe.

610 5.1.3 Power and air conditioning

611 The online machine operates in an air conditioned environment and is not
612 rebooted or power-cycled except for essential maintenance.

613 The signing machine is switched off between signing operations. The machine
614 operates in an air conditioned environment.

615 **5.1.4 Water exposures**

616 No stipulation.

617 **5.1.5 Fire prevention and protection**

618 No stipulation.

619 **5.1.6 Media storage**

620 No stipulation.

621 **5.1.7 Waste disposal**

622 No stipulation.

623 **5.1.8 Off-site backup**

624 No stipulation.

625 **5.2 Procedural Controls**

626 **5.2.1 Trusted roles**

627 No stipulation.

628 **5.2.2 Number of persons required per task**

629 No stipulation.

630 **5.2.3 Identification and authentication for each role**

631 No stipulation.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

- The CA Manager must be a paid employee of CCLRC and shall be appointed in writing by the CCLRC Director of e-Science who may at his/her discretion revoke the appointment with no prior notice given.
- The CA Operators must be paid employees of CCLRC and will be appointed by the CA Manager.
- The RA Manager must be a paid employee of the Physical Organisation hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that physical organisation. The RA Manager must be a member of that Department. The OU field of the RA Operator's certificate identifies the Physical Organisation, and the L field identifies the Department where the Manager is appointed. The Authority will make a declaration to the CA Manager in writing on the organisation's headed note paper. The information that must be contained in this letter is defined by the CA Manager.
- The RA Operator must be a paid employee of the site hosting that Registration Authority and will be appointed by the RA Manager concerned. The RA Manager will make a declaration to the CA Manager in writing on the organisation's headed note paper. If the RA Operator is appointed in a different department from the RA Manager then the letter must be countersigned by an authority for the department in which the Operator is appointed. The information that must be contained in this letter is defined by the CA Manager. RA Operators must have certificates and must adhere also to the Subscribers' Obligations.
- An RA Manager may appoint himself/herself as an RA Operator.
- An RA Manager may appoint any number of RA Operators.

5.3.2 Background check procedures

No stipulation.

662 **5.3.3 Training requirements**

663 No stipulation.

664 **5.3.4 Retraining frequency and requirements**

665 No stipulation.

666 **5.3.5 Job rotation frequency and sequence**

667 No stipulation.

668 **5.3.6 Sanctions for unauthorized actions**

669 In the event of unauthorised actions, abuse of authority or unauthorised use
670 of entity systems by the CA or RA Operators, the CA manager may revoke
671 the privileges concerned.

672 **5.3.7 Contracting personnel requirements**

673 No stipulation.

674 **5.3.8 Documentation supplied to personnel**

- 675 • It is the responsibility of the CA Manager to provide the CA Operators
676 with a copy of the “e-Science CA Operator’s Procedure”.
- 677 • It is the responsibility of the CA Manager to provide the RA Manager
678 with a copy of the “e-Science RA Manager’s Procedure”.
- 679 • It is the responsibility of the RA Manager to provide the RA Operator
680 with a copy of the “e-Science RA Operator’s Procedure”.

681 Chapter 6

682 TECHNICAL SECURITY 683 CONTROLS

684 6.1 Key Pair Generation and Installation

685 6.1.1 Key pair generation

686 Each entity should take reasonable steps to ensure that the key pair is gener-
687 ated with a sufficiently high entropy (i.e. corresponding to the key length.)

688 6.1.2 Private key delivery to entity

689 Each Subscriber must generate his/her own key pair. The CA does not
690 generate private keys for its subscribers.

691 6.1.3 Public key delivery to certificate issuer

692 Subscribers' public keys are delivered to the issuing CA by the HTTP pro-
693 tocol via the CA's web interface.

694 6.1.4 CA public key delivery to subscribers

695 The CA certificate (containing its public key) is delivered to subscribers by
696 online transaction from the CA web server.

6.1.5 Key sizes

Keys of length less than 1024 bits are not accepted. The CA key is of length 2048 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

No stipulation.

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

Keys may be used for authentication, non-repudiation, data encryption, message integrity and session key establishment.

The CA's private key is the only key that can be used for signing certificates and CRLs.

The certificate KeyUsage field is used in accordance with RFC3280, [HPFS02].

6.2 Private Key Protection**6.2.1 Standards for cryptographic module**

No stipulation.

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

Subscriber's keys must not be under (n out of m) multi-person control. The CA's private key is not under (n out of m) multi-person control.

719 Backup copies of the CA's private key will be under (2 out of 3) multi-
720 person control (as well as locked in a safe as described in 6.2.4). The backup
721 private key can be activated only by two of the following:

- 722 • ~~David BOYD, CCLRC (Deputy Director of the CCLRC e-Science centre)~~
- 723 • ~~Jens G JENSEN, CCLRC (CA Manager)~~
- 724 • ~~Alistair MILLS, CCLRC (CA Operator and Grid Support Centre manager)~~

725 **6.2.3 Private key escrow**

726 Private keys must not be escrowed.

727 **6.2.4 Private key backup**

728 All backup copies of the CA private key are kept at least as secure as the
729 one used for signing (i.e. encrypted, and on media locked in a safe). The
730 pass-phrase for activating the backup is locked in a different safe from the
731 one containing the encrypted key.

732 **6.2.5 Private key archival**

733 No stipulation.

734 **6.2.6 Private key entry into cryptographic module**

735 No stipulation.

736 **6.2.7 Method of activating private key**

737 The CA private key is activated by a pass-phrase which, for emergencies, is
738 kept in a sealed envelope in a safe. The safe which contains the pass-phrase
739 does not contain any copy of the private key.

740 **6.2.8 Method of deactivating private key**

741 No stipulation.

742 **6.2.9 Method of destroying private key**

743 No stipulation.

744 **6.3 Other Aspects of Key Pair Management**

745 **6.3.1 Public key archival**

746 The CA archives all issued certificates.

747 **6.3.2 Usage periods for the public and private keys**

748 Subscribers' certificates have a validity period of one year. The CA certificate
749 has a validity period of five years.

750 **6.4 Activation Data**

751 The CA private key is protected by a Strong Pass-phrase.

752 **6.4.1 Activation data generation and installation**

753 No stipulation.

754 **6.4.2 Activation data protection**

755 All CA Operators know the Activation Data for the CA private key. No
756 other person knows the Activation Data. However, the Activation Data for
757 the CA private key is also kept in a sealed envelope in a safe in a separate
758 location from the safes containing the private key and its backup copies.

759 **6.4.3 Other aspects of activation data**

760 No stipulation.

761 **6.5 Computer Security Controls**

762 **6.5.1 Specific computer security technical requirements**

763 The CA server includes the following functionality:

- 764 • operating systems are maintained at a high level of security by applying
765 in a timely manner all recommended and applicable security patches;
- 766 • monitoring is done to detect unauthorised software changes;
- 767 • services are reduced to the bare minimum.

768 **6.5.2 Computer security rating**

769 No stipulation.

770 **6.6 Life-Cycle Technical Controls**

771 **6.6.1 System development controls**

772 System development is done on mirror machines containing the same software
773 but no production data.

774 **6.6.2 Security management controls**

775 No stipulation.

776 **6.6.3 Life cycle security ratings**

777 No stipulation.

778 **6.7 Network Security Controls**

779 Certificates are generated on a machine not connected to any kind of network,
780 located in a secure environment and managed by a suitably trained person.
781 The public machine is protected by a suitably configured firewall.

782 **6.8 Cryptographic Module Engineering Con-**
783 **trols**

784 No stipulation.

785 **Chapter 7**

786 **CERTIFICATE AND CRL**
787 **PROFILES**

788 **7.1 Certificate Profile**

789 **7.1.1 Version number**

790 X.509.v3

791 **7.1.2 Certificate extensions**

792 Server and service certificates have the same extensions.

Basic Constraints	<i>critical</i> , CA:FALSE
Key Usage	<i>critical</i> , Digital Signature, Non Repudiation, Key Encryption, Key Agreement
Subject Key Identifier	hash
Authority Key Identifier	keyid, issuer
Subject Alternative Name (server/service only)	Server's Fully Qualified Domain Name

Issuer Name	Alternative	CA email
CRL Points	Distribution	[CAC]
Netscape Cert Type		Personal: SSL Client, S/MIME Server, service: SSL Client, SSL Server
Netscape Comment		“UK e-Science User Certificate”
Netscape CA Revocation URL		[CAC]
Netscape Revocation URL		[CAC]
Netscape URL	Renewal	http://ca-renew.grid-support.ac.uk/renew.html

793 CA certificate extensions.

Basic Constraints		<i>critical</i> CA:TRUE
Key Usage		keyCertSign, cRLSign
Subject Key Identifier		hash
Authority Key Identifier		keyid, issuer
Subject Name	Alternative	CA email
Issuer Name	Alternative	CA email

CRL Distribution Points	[CAC]
Netscape Cert Type	SSL CA, S/MIME CA

794 7.1.3 Algorithm object identifiers

795 No stipulation.

796 7.1.4 Name forms

797 Issuer (as seen with OpenSSL versions 0.9.6 and earlier):

798 /C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-
799 support.ac.uk

800 Issuer as seen with OpenSSL version 0.9.7:

801
802 /C=UK/O=eScience/OU=Authority/CN=CA/emailAddress=ca-operator@grid-support.ac.uk

803 Subject: The subject field contains the Distinguished Name of the entity
804 with the following attributes:

Country Name	UK
Organisation Name	eScience
Organizational Unit	Name of physical organisation hosting the RA approving the Subject's request
Locality	Location within the organisation where the RA is appointed.
CommonName	Name and surname (personal and object-signing certificates) or DNS name (server certificates). Grid service certificates are prefixed by the service name (see 7.1.5) by / (e.g. CN=ldap/ldap.rl.ac.uk).

SubjectAltName	FQDN of server
----------------	----------------

805 **7.1.5 Name constraints**

806 The email address in server and service certificates must be that of a person
807 responsible for the server in question. Server (host) certificates should not
808 have “host” as a service, i.e. they should have `CN=host.univ.ac.uk` and not
809 `CN=host/host.univ.ac.uk`.

810 The CA will issue certificates for a given service if and only if:

- 811 • the service has been defined by IANA [IAN]; or
- 812 • The CA Manager has approved the service.

813 It is the responsibility of the CA Manager to define the non-IANA services
814 allowed by the CA. For each service, the CA Manager must provide

- 815 • the name of the service,
- 816 • the default port number,
- 817 • a short description of the service,
- 818 • a reference URI.

819 The CA Manager must ensure that services are unique in name.

820 **7.1.6 Certificate policy Object Identifier**

821 No stipulation.

822 **7.1.7 Usage of Policy Constraints extensions**

823 No stipulation.

824 **7.1.8 Policy qualifier syntax and semantics**

825 No stipulation.

826 **7.1.9 Processing semantics for the critical certificate**
827 **policy**

828 No stipulation.

829 **7.2 CRL Profile**

830 **7.2.1 Version number**

831 X.509.v1: Version 1 is required for compatibility with Netscape Communi-
832 cator.

833 **7.2.2 CRL and CRL Entry Extensions**

834 No stipulation.

835 Chapter 8

836 SPECIFICATION 837 ADMINISTRATION

838 8.1 Specification Change Procedures

839 We distinguish between different types of modifications to the CP/CPS:

840 *Editorial updates:* editorial changes to the CPS, including replacing fields
841 with “No stipulation”, as long as they do not affect procedure or compromise
842 security. These changes are announced on the CA web site but no advance
843 warning will be given.

844 *Procedure updates:* minor changes to the CPS that do not compromise secu-
845 rity in any way. E.g. changes to the verification or issuing procedure that
846 do not affect security. Subscribers and relying parties will not be warned of
847 such changes in advance but RAs will be given at least one week’s notice of
848 changes that affect their procedures.

849 *Technical updates:* e.g. changes to the extensions in the issued certificates.
850 Such changes will be announced on the CA web site and on appropriate
851 mailing lists at least 14 days in advance.

852 *Security updates:* changes that affect the security, e.g. changes to the minimal
853 requirements for verifying requests, or changing the key sizes. These changes
854 will be announced at least 30 days in advance on the CA web site, and to
855 appropriate mailing lists, including the DataGrid CA mailing list. However,
856 urgent security fixes may be carried out without advance warning and then
857 documented in the CPS. These will be announced in the same manner.

858 *Policy updates:* e.g. changes to the namespace, or introducing subordinate
859 CAs. A proposal will be announced at least 30 days in advance on the CA

860 web site and appropriate mailing lists.

861 *Termination:* A scheduled termination of the CA is announced on the CA
862 web site and appropriate mailing lists at least 60 days in advance.

863 **8.2 Publication and Notification Policies**

864 This CP/CPS is available at [CAW]. All changes are announced on the CA
865 web site and a changelog is available. In addition, changes are announced to
866 appropriate mailing lists, depending on the type of change, as described in
867 section 8.1.

868 There is a mailing list for RA Managers and Operators. Only subscribers
869 can post to the mailing list. Only subscribers can read the archives.

870 **8.3 CPS Approval Procedures**

871 No stipulation.

872 Appendix A

873 Revision History

Version	OID	Date	Comments
0.1		4 September 2001	Initial unapproved release
0.3		30 January 2002	Andrew's changes
0.4		13 March 2002	Jens' changes
0.5		April/May 2002	Tim's changes
0.6		28 May 2002	draft version
0.7	1.1	17 July 2002	final draft
0.8	1.2	10 October 2002	Removed identification by telephone, made specification of host verification more precise, added missing RFC2527 entries.
0.9	1.3	31 March 2003	Update to request extensions.
1.0	1.4	30 October 2003	Describe renewal. Tightened up several parts, including Applicability, personal information stored, etc.
1.1	1.5		More about the data protection act.

874

⁸⁷⁵ The OID in the table is the final two digits of the actual OID, as defined in
⁸⁷⁶ section 1.2.

877 Bibliography

- 878 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate
879 policy model. http://www.gridforum.org/2_SEC/pdf/Draft-
880 GGF-CP-06.pdf, September 2001.
- 881 [CAC] CA Certificate Revocation List. <http://ca.grid-support.ac.uk/->
882 [cgi-bin/importCRL](http://ca.grid-support.ac.uk/-cgi-bin/importCRL).
- 883 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 884 [Cec01] R. Cecchini. INFN CA CP/CPS. <http://security.fi.infn.it/CA/->
885 [CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/-CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 886 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-
887 ture Certificate Policy and Certification Practices Framework.
888 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 889 [CFS+03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet
890 x.509 public key infrastructure certificate policy and certification
891 practices framework. <http://www.ietf.org/internet-drafts/draft->
892 [ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 893 [DPA00] Data protection act 1998. <http://www.legislation.hmso.gov.uk/->
894 [acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/-acts/acts1998/19980029.htm), March 2000.
- 895 [Eur00] EuroPKI Certificate Policy. <http://www.europki.org/ca/root/->
896 [cps/en_cp.pdf](http://www.europki.org/ca/root/-cps/en_cp.pdf), October 2000. Version 1.1.
- 897 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-
898 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,
899 December 1999. Version 1.0.
- 900 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.
901 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.
902 Version 1.1.

- 903 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.
904 <http://www.globus.org/security/v2.0/index.html>.
- 905 [Glob] Globus. Grid security infrastructure for globus toolkit 3.
906 <http://www.globus.org/security/GSI3/index.html>.
- 907 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 908 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String
909 Representation of Standard Attribute Syntaxes. [http://www.rfc-](http://www.rfc-editor.org/rfc/rfc1778.txt)
910 [editor.org/rfc/rfc1778.txt](http://www.rfc-editor.org/rfc/rfc1778.txt), March 1995.
- 911 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public
912 key infrastructure certificate and certificate revocation list (crl)
913 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 914 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 915 [NCS99] National Computational Science Alliance Certificate Pol-
916 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html)
917 [Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html), June 1999.
- 918 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-](http://www.digsigtrust.com/-certificates/policy/tsindex.html)
919 [certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 920 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight
921 Directory Access Protocol (v3): Attribute Syntax Definitions.
922 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.