



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

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

04 March 2005

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 . . . 17

- 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	51
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	52
6.5.1	Specific computer security technical requirements	52
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	53
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	59
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 1.0 AND 1.1. IT IS NOT A VALID CP/CPS. IT
9 DOCUMENTS CHANGES BETWEEN THE VERSIONS.

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

13 1.1.1 General definitions

14 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).
GSI	Grid Security Infrastructure. In this document, GSI refers to the Globus GSI as defined in [Gloa] or [Glob].
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.
SSL	Secure Sockets Layer. In this document, “SSL” refers to the SSL protocol version 2 or 3, or TLS version 1.0 (RFC2246).

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).

15 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	<u>Changelog between 1.0 and 1.1</u>

16 The document OID is {iso(1) identified-organization(3) dod(6) internet(1)
 17 private(4) enterprise(1) cclrc(11439) 1 escience(1) ca(1) cps(1)
 18 5}.

19 See also revision history in Appendix A.

20 **1.3 Community and Applicability**

21 **1.3.1 Certification authorities**

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

24 **1.3.2 Registration authorities**

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

32 **1.3.3 End entities (Subscribers)**

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

35 **1.3.4 Applicability**

36 Certificates issued are suitable for the following applications:

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

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

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

46 **1.4 Contact Details**

47 **1.4.1 Specification administration organisation**

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

49 **1.4.2 Contact person**

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

52 Dr Jens G Jensen
53 Rutherford Appleton Laboratory
54 Chilton
55 Didcot
56 Oxon
57 OX11 0QX
58 UK
59
60 Phone: +44 1 235 446104
61 Fax: +44 1 235 445945
62 Email: ca-manager@grid-support.ac.uk

63 **1.4.3 Person determining CPS suitability for the pol-
64 icy**

65 The person mentioned in 1.4.2.

66 Chapter 2

67 GENERAL PROVISIONS

68 2.1 Obligations

69 2.1.1 CA obligations

70 The CA must:

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

85 **2.1.2 RA obligations**

86 The RA Manager must:

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

102 The RA Operator must:

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

- 115 • sign Subscriber's request when and only when all conditions for issuing
116 a certificate to the Subscriber are fulfilled;
- 117 • Request revocation of a Subscriber's certificate when and only when
118 the RA Operator is aware that (1) the circumstances for revocation
119 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

120 **2.1.3 Subscriber obligations**

121 Subscribers must:

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

137 **2.1.4 Relying party obligations**

138 A Relying Party should accept the Subscriber's certificate for authentication
139 purposes if:

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

- 143 • the reliance is reasonable and in good faith in light of all circumstances
144 known to the Relying Party at the time of reliance; and
- 145 • the certificate is used for permitted purposes only; and
- 146 • the Relying Party checked the status of the certificate to their own
147 satisfaction prior to reliance.

148 **2.1.5 Repository obligations**

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

151 **2.2 Liability**

152 **2.2.1 CA liability**

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

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

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

168 **2.2.2 RA liability**

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

173 **2.3 Financial Responsibility**

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

175 **2.3.1 Indemnification by relying parties**

176 No stipulation.

177 **2.3.2 Fiduciary relationships**

178 No stipulation.

179 **2.3.3 Administrative processes**

180 No stipulation.

181 **2.4 Interpretation and Enforcement**

182 **2.4.1 Governing law**

183 Interpretation of this policy is according to UK Law.

184 **2.4.2 Severability, survival, merger, notice**

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

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

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

192 **2.4.3 Dispute resolution procedures**

193 No stipulation.

194 **2.5 Fees**

195 **2.5.1 Certificate issuance or renewal fees**

196 No fees are charged for the certification service and therefore there are no
197 financial encumbrances.

198 **2.5.2 Certificate access fees**

199 No fees are charged for certificate access.

200 **2.5.3 Revocation or status information access fees**

201 No fees are charged for access to revocation lists or other certificate status
202 information.

203 **2.5.4 Fees for other services such as policy information**

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

207 **2.5.5 Refund policy**

208 No stipulation.

209 **2.6 Publication and Repositories**

210 **2.6.1 Publication of CA information**

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

- 212 • The e-Science CA's certificate;
- 213 • Certificates issued;
- 214 • Certificate Revocation Lists;

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

218 **2.6.2 Frequency of publication**

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

222 **2.6.3 Access controls**

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

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

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

233 **2.6.4 Repositories**

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

235 **2.7 Compliance Audit**

236 **2.7.1 Frequency of entity compliance audit**

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

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

242 **2.7.2 Identity/qualifications of auditor**

243 No stipulation.

244 **2.7.3 Auditor's relationship to audited party**

245 An external audit can be performed by any UK government department or
246 UK academic institution.

247 **2.7.4 Topics covered by audit**

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

250 **2.7.5 Actions taken as a result of deficiency**

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

253 **2.7.6 Communication of results**

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

256 **2.8 Confidentiality**

257 The e-Science CA collects a subscriber's name and e-mail address. The sub-
258 scriber's name as defined in 3.1.2-3, but not e-mail address, is included in
259 the issued personal certificate (server certificates include email address). In
260 addition, the RA keeps a copy of the photo id that was used by the Sub-
261 scriber to verify his/her identity. By making an application for a certificate
262 a Subscriber is deemed to have consented to their personal data being stored
263 and processed, subject to the Data Protection Act 1998.

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

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

268 **2.8.1 Types of information to be kept confidential**

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

273 **2.8.2 Types of information not considered confidential**

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

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

279 **2.8.3 Disclosure of certificate revocation/suspension in-** 280 **formation**

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

283 **2.8.4 Release to law enforcement officials**

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

287 **2.8.5 Release as part of civil discovery**

288 No stipulation.

289 **2.8.6 Disclosure upon owner's request**

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

294 The CA will recognise requests in writing for the release of personal infor-
295 mation from a Subscriber provided the Subscriber can be properly authen-
296 ticated. The CA reserves the right to charge a reasonable fee for the service
297 in this case.

298 **2.8.7 Other information release circumstances**

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

301 **2.9 Intellectual Property Rights**

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

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

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

309 This document typeset with L^AT_EX.

310 Chapter 3

311 IDENTIFICATION AND 312 AUTHENTICATION

313 3.1 Initial Registration

314 3.1.1 Types of names

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

318 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.

319
320 Common Names (CNs) must be encoded as `PrintableStrings` ([WCHK97],[HKYR95]).

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

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

323 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

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

328 Email address in server and service certificates must be structured accord-
 329 ing to RFC822. The maximal length of an email address is 128 characters.
 330 Email addresses must be encoded as `IA5String` but must not contain control
 331 characters or delete.

332 See also 7.1.4.

333 3.1.2 Need for names to be meaningful

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

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

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

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

342 This certificate is used only within the CA by CA Operators for CA main-
 343 tenance, i.e. to allow CA Operators the same access to the public system as
 344 RA Operators. This certificate is also used to sign software deployed by the
 345 CA. This certificate is never used for any other purpose; in particular, it is
 346 never used to access any resources other than the CA's public machine.

347 3.1.3 Rules for interpreting various name forms

348 No stipulation.

349 **3.1.4 Uniqueness of names**

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

358 **3.1.5 Name claim dispute resolution procedure**

359 No stipulation.

360 **3.1.6 Recognition, authentication and role of trade-** 361 **marks**

362 No stipulation.

363 **3.1.7 Method to prove possession of private key**

364 No stipulation.

365 **3.1.8 Authentication of organisation identity**

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

369 **3.1.9 Authentication of individual identity**

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

372 In either case the Subscriber selects which RA is to carry out the identi-
373 fication 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).

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

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

387 3.2 Routine Re-key

388 No stipulation.

389 **3.3 Re-key After Revocation**

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

392 **3.4 Revocation Request**

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

397 Authenticated certificate revocation requests may be made by

- 398 • The RA using:
 - 399 – Signed Email to the CA Manager;
 - 400 – Other secure method, as specified in the RA Operator's procedure.
- 401 • The Subscriber by:
 - 402 – Mailing the CA manager directly by Signed Email.

403 Chapter 4

404 OPERATIONAL 405 REQUIREMENTS

406 4.1 Certificate Application

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

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

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

415 4.2 Certificate Issuance

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

419 In the case of renewal, the authentication is considered successful if the
420 DN of the new request matches that of the certificate used by the client when
421 submitting the request. The request needs RA approval to verify that the
422 client is still entitled to a certificate, but the RA need not verify the client's
423 identity.

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

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

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

432 All issued certificates are issued under the CP/CPS valid at the time of
433 issuance.

434 **4.3 Certificate Acceptance**

435 No stipulation.

436 **4.4 Certificate Suspension and Revocation**

437 **4.4.1 Circumstances for revocation**

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

- 441 • The CA is informed that the Subscriber has ceased to be a member of
442 or associated with a UK e-Science program or activity;
- 443 • the Subscriber's private key is lost or suspected to be compromised;
- 444 • the information in the subscriber's certificate is wrong or inaccurate,
445 or suspected to be wrong or inaccurate;
- 446 • the Subscriber violates his/her obligations.

447 **4.4.2 Who can request revocation**

448 A certificate revocation can be requested by:

- 449 • The Registration Authority which authenticated the holder of the cer-
450 tificate;

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

454 **4.4.3 Procedure for revocation request**

455 A revocation request is accepted if:

- 456 • The revocation request is signed with the key corresponding to certifi-
- 457 cate whose revocation is requested; or,
- 458 • The revocation request is signed by the RA who originally approved
- 459 the certificate request.

460 Any other revocation request is accepted only if the entity requesting the
461 revocation is properly authenticated.

462 **4.4.4 Revocation request grace period**

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

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

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

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

473 **4.4.5 Circumstances for suspension**

474 The CA does not offer suspension services.

475 **4.4.6 Who can request suspension**

476 No stipulation.

477 **4.4.7 Procedure for suspension request**

478 No stipulation.

479 **4.4.8 Limits on suspension period**

480 No stipulation.

481 **4.4.9 CRL issuance frequency**

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

484 **4.4.10 CRL checking requirements**

485 No stipulation.

486 **4.4.11 On-line revocation/status checking availability**

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

488 **4.4.12 On-line revocation checking requirements**

489 No stipulation.

490 **4.4.13 Other forms of revocation advertisements avail-**
491 **able**

492 No stipulation.

493 **4.4.14 Checking requirements for other forms of revo-**
494 **cation advertisements**

495 No stipulation.

496 **4.4.15 Special requirements re key compromise**

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

501 **4.5 Security Audit Procedures**

502 **4.5.1 Types of event recorded**

503 The following events are recorded:

- 504 • certification requests;
- 505 • issued certificates;
- 506 • requests for revocation;
- 507 • issued CRLs;
- 508 • login/logout/reboot of the signing machine.

509 **4.5.2 Frequency of processing log**

510 No stipulation.

511 **4.5.3 Retention period for audit log**

512 The minimum retention period is 3 years.

513 **4.5.4 Protection of audit log**

514 No stipulation.

515 **4.5.5 Audit log backup procedures**

516 No stipulation.

517 4.5.6 Audit collection system (internal vs external)

518 No stipulation.

519 4.5.7 Notification to event-causing subject

520 No stipulation.

521 4.5.8 Vulnerability assessments

522 No stipulation.

523 4.6 Records Archival**524 4.6.1 Types of event recorded**

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

- 526 • certification requests;
- 527 • issued certificates;
- 528 • requests for revocation;
- 529 • issued CRLs;
- 530 • all e-mail messages received by the CA (not the confirmation messages
531 sent to the Subscribers);
- 532 • all e-mail messages sent by the CA;
- 533 • all documents appointing CA and RA Staff.

534 Each RA must log the following:

- 535 • for each approved request, how it was approved;
- 536 • for each rejected request, why it was rejected;
- 537 • for each approved revocation request, the reason for revocation;
- 538 • for each rejected revocation request, the reason for revocation and the
539 reason the request was rejected.

540 **4.6.2 Retention period for archive**

541 The minimum retention period is 3 years.

542 **4.6.3 Protection of archive**

543 No stipulation.

544 **4.6.4 Archive backup procedures**

545 No stipulation.

546 **4.6.5 Requirements for time-stamping of records**

547 No stipulation.

548 **4.6.6 Archive collection system (internal or external)**

549 No stipulation.

550 **4.6.7 Procedures to obtain and verify archive information**
551 **tion**

552 No stipulation.

553 **4.7 Key Changeover**

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

558 **4.8 Compromise and Disaster Recovery**

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

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

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

567 **4.8.1 Computing resources, software, and/or data are** 568 **corrupted**

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

570 **4.8.2 Entity public key is revoked**

571 No stipulation.

572 **4.8.3 Entity key is compromised**

573 No stipulation.

574 **4.8.4 Secure facility after a natural or other type of** 575 **disaster**

576 No stipulation.

577 **4.9 CA Termination**

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

- 579 • inform the Registration Authorities, Subscribers, Relying Parties, and
580 cross-certifying CAs of which the CA is aware;
- 581 • make information of its termination widely available;
- 582 • stop issuing certificates.

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

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

593 Chapter 5

594 PHYSICAL, PROCEDURAL, 595 AND PERSONNEL 596 SECURITY CONTROLS

597 5.1 Physical Controls

598 5.1.1 Site location and construction

599 No stipulation.

600 5.1.2 Physical access

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

604 5.1.3 Power and air conditioning

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

607 The signing machine is switched off between signing operations. The machine
608 operates in an air conditioned environment.

609 **5.1.4 Water exposures**

610 No stipulation.

611 **5.1.5 Fire prevention and protection**

612 No stipulation.

613 **5.1.6 Media storage**

614 No stipulation.

615 **5.1.7 Waste disposal**

616 No stipulation.

617 **5.1.8 Off-site backup**

618 No stipulation.

619 **5.2 Procedural Controls**

620 **5.2.1 Trusted roles**

621 No stipulation.

622 **5.2.2 Number of persons required per task**

623 No stipulation.

624 **5.2.3 Identification and authentication for each role**

625 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.

656 **5.3.3 Training requirements**

657 No stipulation.

658 **5.3.4 Retraining frequency and requirements**

659 No stipulation.

660 **5.3.5 Job rotation frequency and sequence**

661 No stipulation.

662 **5.3.6 Sanctions for unauthorized actions**

663 In the event of unauthorised actions, abuse of authority or unauthorised use
664 of entity systems by the CA or RA Operators, the CA manager may revoke
665 the privileges concerned.

666 **5.3.7 Contracting personnel requirements**

667 No stipulation.

668 **5.3.8 Documentation supplied to personnel**

- 669 • It is the responsibility of the CA Manager to provide the CA Operators
670 with a copy of the “e-Science CA Operator’s Procedure”.
- 671 • It is the responsibility of the CA Manager to provide the RA Manager
672 with a copy of the “e-Science RA Manager’s Procedure”.
- 673 • It is the responsibility of the RA Manager to provide the RA Operator
674 with a copy of the “e-Science RA Operator’s Procedure”.

675 Chapter 6

676 TECHNICAL SECURITY 677 CONTROLS

678 6.1 Key Pair Generation and Installation

679 6.1.1 Key pair generation

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

682 6.1.2 Private key delivery to entity

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

685 6.1.3 Public key delivery to certificate issuer

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

688 6.1.4 CA public key delivery to subscribers

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

691 **6.1.5 Key sizes**

692 Keys of length less than 1024 bits are not accepted. The CA key is of length
693 2048 bits.

694 **6.1.6 Public key parameters generation**

695 No stipulation.

696 **6.1.7 Parameter quality checking**

697 No stipulation.

698 **6.1.8 Hardware/software key generation**

699 No stipulation.

700 **6.1.9 Key usage purposes (as per X.509 v3 key usage 701 field)**

702 Keys may be used for authentication, non-repudiation, data encryption, mes-
703 sage integrity and session key establishment.

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

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

707 **6.2 Private Key Protection**

708 **6.2.1 Standards for cryptographic module**

709 No stipulation.

710 **6.2.2 Private key (n out of m) multi-person control**

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

713 Backup copies of the CA's private key is under (2 out of 3) multi-person
714 control (as well as locked in a safe as described in 6.2.4).

715 **6.2.3 Private key escrow**

716 Private keys must not be escrowed.

717 **6.2.4 Private key backup**

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

722 **6.2.5 Private key archival**

723 No stipulation.

724 **6.2.6 Private key entry into cryptographic module**

725 No stipulation.

726 **6.2.7 Method of activating private key**

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

730 **6.2.8 Method of deactivating private key**

731 No stipulation.

732 **6.2.9 Method of destroying private key**

733 No stipulation.

734 **6.3 Other Aspects of Key Pair Management**

735 **6.3.1 Public key archival**

736 The CA archives all issued certificates.

737 **6.3.2 Usage periods for the public and private keys**

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

740 **6.4 Activation Data**

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

742 **6.4.1 Activation data generation and installation**

743 No stipulation.

744 **6.4.2 Activation data protection**

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

749 **6.4.3 Other aspects of activation data**

750 No stipulation.

751 **6.5 Computer Security Controls**

752 **6.5.1 Specific computer security technical requirements**

753 The CA server includes the following functionality:

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

758 **6.5.2 Computer security rating**

759 No stipulation.

760 **6.6 Life-Cycle Technical Controls**

761 **6.6.1 System development controls**

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

764 **6.6.2 Security management controls**

765 No stipulation.

766 **6.6.3 Life cycle security ratings**

767 No stipulation.

768 **6.7 Network Security Controls**

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

772 **6.8 Cryptographic Module Engineering Con-** 773 **controls**

774 No stipulation.

775 Chapter 7

776 CERTIFICATE AND CRL 777 PROFILES

778 7.1 Certificate Profile

779 7.1.1 Version number

780 X.509.v3

781 7.1.2 Certificate extensions

782 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
Signature Algorithm		<u>sha1WithRSAEncryption</u>

783 CA certificate extensions.

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

Issuer Name	Alternative	CA email
CRL Points	Distribution	[CAC]
Netscape Cert Type		SSL CA, S/MIME CA
<u>Signature Algorithm</u>		<u>sha1WithRSAEncryption</u>

784 7.1.3 Algorithm object identifiers

785 No stipulation.

786 7.1.4 Name forms

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

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

790 Issuer as seen with OpenSSL version 0.9.7:

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

793 Subject: The subject field contains the Distinguished Name of the entity
794 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

795 **7.1.5 Name constraints**

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

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

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

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

- 805 • the name of the service,
- 806 • the default port number,
- 807 • a short description of the service,
- 808 • a reference URI.

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

810 **7.1.6 Certificate policy Object Identifier**

811 No stipulation.

812 **7.1.7 Usage of Policy Constraints extensions**

813 No stipulation.

814 **7.1.8 Policy qualifier syntax and semantics**

815 No stipulation.

816 **7.1.9 Processing semantics for the critical certificate**
817 **policy**

818 No stipulation.

819 **7.2 CRL Profile**

820 **7.2.1 Version number**

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

823 **7.2.2 CRL and CRL Entry Extensions**

824 No stipulation.

825 Chapter 8

826 SPECIFICATION 827 ADMINISTRATION

828 8.1 Specification Change Procedures

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

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

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

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

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

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

850 web site and appropriate mailing lists.

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

853 **8.2 Publication and Notification Policies**

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

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

860 **8.3 CPS Approval Procedures**

861 No stipulation.

862 Appendix A

863 Revision History

864

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. Describe renewal. Tightened
1.0	1.4	30 October 2003	up several parts, including Applicability, personal information stored, etc.
1.1	1.5	04 March 2005	Documented that we use SHA1 to sign.

865

⁸⁶⁶ The OID in the table is the final two digits of the actual OID, as defined in
⁸⁶⁷ section 1.2.

868 Bibliography

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

- 894 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.
895 <http://www.globus.org/security/v2.0/index.html>.
- 896 [Glob] Globus. Grid security infrastructure for globus toolkit 3.
897 <http://www.globus.org/security/GSI3/index.html>.
- 898 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 899 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String
900 Representation of Standard Attribute Syntaxes. <http://www.rfc-editor.org/rfc/rfc1778.txt>, March 1995.
901
- 902 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public
903 key infrastructure certificate and certificate revocation list (crl)
904 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 905 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 906 [NCS99] National Computational Science Alliance Certificate Pol-
907 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html)
908 [Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html), June 1999.
- 909 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-](http://www.digsigtrust.com/-certificates/policy/tsindex.html)
910 [certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 911 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight
912 Directory Access Protocol (v3): Attribute Syntax Definitions.
913 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.