



UK e-Science Certification Authority
Certificate Policy and Certification Practices
Statement
Version 1.2

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

15 May 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) 17
 - 1.3.4 Applicability 17
 - 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 22
 - 2.1.5 Repository obligations 22
 - 2.2 Liability 23
 - 2.2.1 CA liability 23
 - 2.2.2 RA liability 23
 - 2.3 Financial Responsibility 23

2.3.1	Indemnification by relying parties	23
2.3.2	Fiduciary relationships	23
2.3.3	Administrative processes	24
2.4	Interpretation and Enforcement	24
2.4.1	Governing law	24
2.4.2	Severability, survival, merger, notice	24
2.4.3	Dispute resolution procedures	24
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	25
2.5.4	Fees for other services such as policy information	25
2.5.5	Refund policy	25
2.6	Publication and Repositories	25
2.6.1	Publication of CA information	25
2.6.2	Frequency of publication	25
2.6.3	Access controls	26
2.6.4	Repositories	26
2.7	Compliance Audit	26
2.7.1	Frequency of entity compliance audit	26
2.7.2	Identity/qualifications of auditor	26
2.7.3	Auditor's relationship to audited party	27
2.7.4	Topics covered by audit	27
2.7.5	Actions taken as a result of deficiency	27
2.7.6	Communication of results	27
2.8	Confidentiality	27
2.8.1	Types of information to be kept confidential	28
2.8.2	Types of information not considered confidential	28
2.8.3	Disclosure of certificate revocation/suspension information	28
2.8.4	Release to law enforcement officials	28
2.8.5	Release as part of civil discovery	28
2.8.6	Disclosure upon owner's request	28

2.8.7 Other information release circumstances 29
2.9 Intellectual Property Rights 29

3 IDENTIFICATION AND AUTHENTICATION 31

3.1 Initial Registration 31
3.1.1 Types of names 31
3.1.2 Need for names to be meaningful 32
3.1.3 Rules for interpreting various name forms 32
3.1.4 Uniqueness of names 33
3.1.5 Name claim dispute resolution procedure 33
3.1.6 Recognition, authentication and role of trademarks 33
3.1.7 Method to prove possession of private key 33
3.1.8 Authentication of organisation identity 33
3.1.9 Authentication of individual identity 34
3.2 Routine Re-key 34
3.3 Re-key After Revocation 34
3.4 Revocation Request 35

4 OPERATIONAL REQUIREMENTS 37

4.1 Certificate Application 37
4.2 Certificate Issuance 37
4.3 Certificate Acceptance 38
4.4 Certificate Suspension and Revocation 38
4.4.1 Circumstances for revocation 38
4.4.2 Who can request revocation 38
4.4.3 Procedure for revocation request 39
4.4.4 Revocation request grace period 39
4.4.5 Circumstances for suspension 39
4.4.6 Who can request suspension 39
4.4.7 Procedure for suspension request 40
4.4.8 Limits on suspension period 40
4.4.9 CRL issuance frequency 40
4.4.10 CRL checking requirements 40
4.4.11 On-line revocation/status checking availability 40

4.4.12	On-line revocation checking requirements	40
4.4.13	Other forms of revocation advertisements available . . .	40
4.4.14	Checking requirements for other forms of revocation advertisements	40
4.4.15	Special requirements re key compromise	41
4.5	Security Audit Procedures	41
4.5.1	Types of event recorded	41
4.5.2	Frequency of processing log	41
4.5.3	Retention period for audit log	41
4.5.4	Protection of audit log	41
4.5.5	Audit log backup procedures	41
4.5.6	Audit collection system (internal vs external)	42
4.5.7	Notification to event-causing subject	42
4.5.8	Vulnerability assessments	42
4.6	Records Archival	42
4.6.1	Types of event recorded	42
4.6.2	Retention period for archive	43
4.6.3	Protection of archive	43
4.6.4	Archive backup procedures	43
4.6.5	Requirements for time-stamping of records	43
4.6.6	Archive collection system (internal or external)	43
4.6.7	Procedures to obtain and verify archive information . . .	43
4.7	Key Changeover	43
4.8	Compromise and Disaster Recovery	43
4.8.1	Computing resources, software, and/or data are cor- rupted	44
4.8.2	Entity public key is revoked	44
4.8.3	Entity key is compromised	44
4.8.4	Secure facility after a natural or other type of disaster .	44
4.9	CA Termination	44
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECUR- RITY CONTROLS	47
5.1	Physical Controls	47

5.1.1	Site location and construction	47
5.1.2	Physical access	47
5.1.3	Power and air conditioning	47
5.1.4	Water exposures	48
5.1.5	Fire prevention and protection	48
5.1.6	Media storage	48
5.1.7	Waste disposal	48
5.1.8	Off-site backup	48
5.2	Procedural Controls	48
5.2.1	Trusted roles	48
5.2.2	Number of persons required per task	48
5.2.3	Identification and authentication for each role	48
5.3	Personnel Controls	49
5.3.1	Background, qualifications, experience, and clearance requirements	49
5.3.2	Background check procedures	49
5.3.3	Training requirements	50
5.3.4	Retraining frequency and requirements	50
5.3.5	Job rotation frequency and sequence	50
5.3.6	Sanctions for unauthorized actions	50
5.3.7	Contracting personnel requirements	50
5.3.8	Documentation supplied to personnel	50
6	TECHNICAL SECURITY CONTROLS	51
6.1	Key Pair Generation and Installation	51
6.1.1	Key pair generation	51
6.1.2	Private key delivery to entity	51
6.1.3	Public key delivery to certificate issuer	51
6.1.4	CA public key delivery to subscribers	51
6.1.5	Key sizes	52
6.1.6	Public key parameters generation	52
6.1.7	Parameter quality checking	52
6.1.8	Hardware/software key generation	52

6.1.9	Key usage purposes (as per X.509 v3 key usage field)	52
6.2	Private Key Protection	52
6.2.1	Standards for cryptographic module	52
6.2.2	Private key (n out of m) multi-person control	52
6.2.3	Private key escrow	53
6.2.4	Private key backup	53
6.2.5	Private key archival	53
6.2.6	Private key entry into cryptographic module	53
6.2.7	Method of activating private key	53
6.2.8	Method of deactivating private key	53
6.2.9	Method of destroying private key	53
6.3	Other Aspects of Key Pair Management	54
6.3.1	Public key archival	54
6.3.2	Usage periods for the public and private keys	54
6.4	Activation Data	54
6.4.1	Activation data generation and installation	54
6.4.2	Activation data protection	54
6.4.3	Other aspects of activation data	54
6.5	Computer Security Controls	54
6.5.1	Specific computer security technical requirements	54
6.5.2	Computer security rating	55
6.6	Life-Cycle Technical Controls	55
6.6.1	System development controls	55
6.6.2	Security management controls	55
6.6.3	Life cycle security ratings	55
6.7	Network Security Controls	55
6.8	Cryptographic Module Engineering Controls	55
7	CERTIFICATE AND CRL PROFILES	57
7.1	Certificate Profile	57
7.1.1	Version number	57
7.1.2	Certificate extensions	57
7.1.3	Algorithm object identifiers	59

<i>CONTENTS</i>	9
7.1.4 Name forms	59
7.1.5 Name constraints	60
7.1.6 Certificate policy Object Identifier	60
7.1.7 Usage of Policy Constraints extensions	60
7.1.8 Policy qualifier syntax and semantics	61
7.1.9 Processing semantics for the critical certificate policy .	61
7.2 CRL Profile	61
7.2.1 Version number	61
7.2.2 CRL and CRL Entry Extensions	61
8 SPECIFICATION ADMINISTRATION	63
8.1 Specification Change Procedures	63
8.2 Publication and Notification Policies	64
8.3 CPS Approval Procedures	64
A Revision History	65
B Compliance with Laws and Regulations	69
B.1 The Data Protection Act	69
B.1.1 Definitions	69
B.1.2 Preliminaries	70
B.1.3 Data	70
B.1.4 Consent	71
B.1.5 Processing	71
B.1.6 Purpose	72
B.1.7 Data Release	73
B.1.8 Data Maintenance	73
B.1.9 Data Retention	74
B.1.10 Data Termination	74

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 was issued on 1 May 2005, updated on 9 May 2005, and
8 took effect on 15 March 2005.

9 1.1.1 General definitions

10 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.
Personal Information	For the purpose of this document, Personal Information refers to data which is sufficient for the Identification of a Subscriber according to section 3.1.9. Personal Information will always contain a photo of the individual sufficient for Validation of the Subscriber, and the Subscriber's name sufficient to establish reasonable link to the CN according to section 3.1.2.
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 UK 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 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.

11 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	Version 1.2
Document date	01 May 2005
Effective from	15 May 2005
Document OID	1.3.6.1.4.1.11439.1.1.1.1.6

12 The document OID is {iso(1) identified-organization(3) dod(6) internet(1)
 13 private(4) enterprise(1) cclrc(11439) 1 escience(1) ca(1) cps(1)
 14 6}.

15 See also revision history in Appendix A.

16 Throughout this document “CA” refers to the Issuing Certification Au-
 17 thority; “UK e-Science CA” or “e-Science CA” refer to the whole authority
 18 comprising the CA and all RAs.

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 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. Encryption
41 is not a permitted purpose.

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

44 **1.4 Contact Details**

45 **1.4.1 Specification administration organisation**

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

47 **1.4.2 Contact person**

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

50 Dr Jens G Jensen
51 Rutherford Appleton Laboratory
52 Chilton
53 Didcot
54 Oxon
55 OX11 0QX
56 UK

57

58 Phone: +44 1 235 446104

59 Fax: +44 1 235 445945

60 Email: ca-manager@grid-support.ac.uk

61 **1.4.3 Person determining CPS suitability for the pol-** 62 **icy**

63 The person mentioned in 1.4.2.

64 Chapter 2

65 GENERAL PROVISIONS

66 2.1 Obligations

67 2.1.1 CA obligations

68 The CA must:

- 69 • publish a CP and a CPS, structured according to RFC2527, [CF99];
- 70 • ensure that operations and infrastructure conform to this CP/CPS;
- 71 • issue certificates to entitled Subscribers based on validated requests
72 from Registration Authorities;
- 73 • notify the Subscriber of the issuing of the certificate;
- 74 • publish a list of the issued certificates;
- 75 • accept revocation requests according to the procedures outlined in this
76 document;
- 77 • authenticate entities requesting the revocation of a certificate;
- 78 • generate and publish Certificate Revocation Lists (CRL) as described
79 in the CPS;
- 80 • identify and publish a list of the services for which service certificates
81 are issued (cf. RFC1738 [BLMM94], section 4);
- 82 • produce a detailed statement of procedure conformant to this CPS and
83 make them available to RA staff.

84 The CA is also an RA. For this purpose, the CA Manager is considered
85 the RA Manager for the CA and must adhere also to the RA Manager's obli-
86 gations. Each CA Operator, when acting as an RA Operator, must adhere
87 also to RA Operators' obligations.

88 2.1.2 RA obligations

89 The RA Manager must:

- 90 • agree the name of the RA (the values of the OU and L in the DN) with
91 the CA Manager;
- 92 • define the community of Subscribers for which the RA will approve
93 requests, and any requirements in addition to those imposed by this
94 CP/CPS;
- 95 • ensure that (s)he is appointed according to the procedures described in
96 this CP/CPS;
- 97 • appoint one or more RA Operators according to the procedures de-
98 scribed in this CP/CPS;
- 99 • ensure that the Operator(s) operate according to the procedures pro-
100 vided by the CA;
- 101 • in particular, ensure that the RA stores all logs and additional Sub-
102 scription information securely in accordance with section B.1, and is re-
103 leased only according to the conditions described in section 2.8.
- 104 • provide access to the logs when requested by the CA.

105 The RA Operator must:

- 106 • adhere to all Subscriber's Obligations (2.1.3)
- 107 • accept certification requests from entitled entities;
- 108 • for personal certificates, verify the identity of the Subscriber and keep
109 a log of how each Subscriber was identified;
- 110 • ensure that DN is unique according to section 3.1.4;
- 111 • for both host and service certificates, verify that the Subscriber is the
112 *responsible system administrator* for the resource identified by the cer-
113 tificate, or authorised by the administrator to apply for a certificate;

- 114 ● check that additional location-specific requirements (if any) are fulfilled
115 (an RA may have more stringent requirements for verifying a request
116 than the minimum requirements set out in this policy document - in
117 that case, the RA's web page should list these requirements);
- 118 ● provide information to the Subscriber on how to properly maintain a
119 certificate and the corresponding private key;
- 120 ● check that the information provided in the certificate request is correct
121 as described in section 3.1.9;
- 122 ● sign Subscriber's request when and only when all conditions for issuing
123 a certificate to the Subscriber are fulfilled;
- 124 ● Request revocation of a Subscriber's certificate when and only when
125 the RA Operator is aware that (1) the circumstances for revocation
126 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

127 **2.1.3 Subscriber obligations**

128 Subscribers must:

- 129 ● read and adhere to the procedures published in this document;
- 130 ● generate a key pair using a trustworthy method;
- 131 ● for personal certificates, choose a unique DN according to section 3.1.4;
- 132 ● for host and service certificates, apply for certificates only for resources
133 for which they are responsible;
- 134 ● for host and service certificates, use an email address in the request
135 which satisfies the requirement that mail sent to that address will
136 reach the Subscriber;
- 137 ● use the certificate for the permitted purposes only;
- 138 ● authorise the processing and conservation of personal data (as required
139 under the Data Protection Act 1998 [DPA00]);
- 140 ● take every precaution to prevent any loss, disclosure or unauthorised
141 access to or use of the private key associated with the certificate, in-
142 cluding:

- 143 – (personal certificates) selecting a Strong Pass-phrase;
- 144 – (personal certificates) protecting the pass-phrase from others;
- 145 – notifying immediately the e-Science CA and any relying parties if
- 146 the private key is lost or compromised;
- 147 – requesting revocation if the Subscriber is no longer entitled to a
- 148 certificate, or if information in the certificate becomes wrong or
- 149 inaccurate.

150 **2.1.4 Relying party obligations**

151 A Relying Party should accept the Subscriber's certificate for authentication
152 purposes if:

- 153 ● the Relying Party is familiar with the CA's CP and the CPS under
- 154 which the certificate was issued before drawing any conclusion on trust
- 155 of the Subscriber's certificate; and
- 156 ● the reliance is reasonable and in good faith in light of all circumstances
- 157 known to the Relying Party at the time of reliance; and
- 158 ● the certificate is used for permitted purposes only; and
- 159 ● the Relying Party checked the validity and status of the certificate to
- 160 their own satisfaction prior to reliance.

161 The Relying Party must:

- 162 ● use the Subscriber's certificates for the permitted purposes only;
- 163 ● use for authorisation purposes either
 - 164 – the Subscriber's full DN; or
 - 165 – only the common root (`/C=UK/O=eScience`); or
 - 166 – for host or service certificates, the CN or parts of the CN.

167 In particular, the RP must not rely on either or both of the OU or L
168 for authorisation purposes.

169 **2.1.5 Repository obligations**

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

172 **2.2 Liability**

173 **2.2.1 CA liability**

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

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

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

189 **2.2.2 RA liability**

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

194 **2.3 Financial Responsibility**

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

196 **2.3.1 Indemnification by relying parties**

197 No stipulation.

198 **2.3.2 Fiduciary relationships**

199 No stipulation.

200 **2.3.3 Administrative processes**

201 No stipulation.

202 **2.4 Interpretation and Enforcement**

203 **2.4.1 Governing law**

204 Interpretation of this policy is according to UK Law.

205 **2.4.2 Severability, survival, merger, notice**

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

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

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

213 **2.4.3 Dispute resolution procedures**

214 No stipulation.

215 **2.5 Fees**

216 **2.5.1 Certificate issuance or renewal fees**

217 No fees are charged for the certification service and therefore there are no
218 financial encumbrances.

219 **2.5.2 Certificate access fees**

220 No fees are charged for certificate access.

221 **2.5.3 Revocation or status information access fees**

222 No fees are charged for access to revocation lists or other certificate status
223 information.

224 **2.5.4 Fees for other services such as policy information**

225 No fees are charged for access to CP and CPS or other CA status informa-
226 tion. The CA reserves the right to charge a fee for the release of Personal
227 Information, as described in section 2.8.6.

228 **2.5.5 Refund policy**

229 No stipulation.

230 **2.6 Publication and Repositories**

231 **2.6.1 Publication of CA information**

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

- 233 • The e-Science CA's certificate;
- 234 • Certificates issued;
- 235 • Certificate Revocation Lists;
- 236 • A copy of the most recent version of this CP/CPS and all previous
237 versions since 0.7;
- 238 • Other relevant information.

239 **2.6.2 Frequency of publication**

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

243 **2.6.3 Access controls**

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

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

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

254 In the future, the e-Science CA may impose the access control on host or
255 service certificate requests that the Subscriber must have a valid personal cer-
256 tificate, and use it to make the host or service certificate requests. Advanced
257 warning not less than 14 days will be given via the CA’s web site.

258 **2.6.4 Repositories**

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

260 **2.7 Compliance Audit**

261 **2.7.1 Frequency of entity compliance audit**

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

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

267 **2.7.2 Identity/qualifications of auditor**

268 No stipulation.

269 **2.7.3 Auditor's relationship to audited party**

270 An external audit can be performed by any UK government department or
271 UK academic institution.

272 **2.7.4 Topics covered by audit**

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

275 **2.7.5 Actions taken as a result of deficiency**

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

278 **2.7.6 Communication of results**

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

281 **2.8 Confidentiality**

282 The e-Science CA collects a Subscriber's name and e-mail address. The Sub-
283 scriber's name as defined in 3.1.2-3, but not e-mail address, is included in
284 the issued personal certificate (server certificates include email address). In
285 addition, the RA keeps a copy of the photo id that was used by the Sub-
286 scriber to verify his/her identity. By making an application for a certificate
287 a Subscriber is deemed to have consented to their personal data being stored
288 and processed, subject to the Data Protection Act 1998 (see section B.1).

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

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

293 **2.8.1 Types of information to be kept confidential**

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

298 **2.8.2 Types of information not considered confidential**

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

302 Statistics regarding certificates issuance and revocation contain no Per-
303 sonal Information and is not considered confidential.

304 **2.8.3 Disclosure of certificate revocation/suspension in-** 305 **formation**

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

308 **2.8.4 Release to law enforcement officials**

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

312 **2.8.5 Release as part of civil discovery**

313 No stipulation.

314 **2.8.6 Disclosure upon owner's request**

315 Disclosure upon owner's request is done according to the Data Protection Act
316 [DPA00], Section 7. Specifically, information is released to the Subscriber
317 if the CA has received a Signed Email from the Subscriber requesting the
318 information (in accordance with [DPA00], section 64 (2)). See also section
319 B.1.7. The CA charges no fee for this.

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

324 **2.8.7 Other information release circumstances**

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

327 **2.9 Intellectual Property Rights**

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

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

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

335 This document typeset with L^AT_EX.

336 Chapter 3

337 IDENTIFICATION AND 338 AUTHENTICATION

339 3.1 Initial Registration

340 3.1.1 Types of names

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

344 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.

345
346 Common Names (CNs) must be encoded as `PrintableStrings` ([WCHK97],[HKYR95]).

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

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

349 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

350 that is, Space (blank), decimal digits, lower and upper case US ASCII letters,
351 left and right round brackets, and hyphen. For host and service certificates,
352 the following characters are permitted:

353 '0' - '9', 'a' - 'z', 'A' - 'Z', '-', '.'

354 that is, digits, US ASCII letters, hyphen, and dot. In addition, names must
355 be structured according to RFC1034 [Moc87]. For service certificates, the
356 character '/' is also allowed in the Common Name.

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

361 See also 7.1.4.

362 **3.1.2 Need for names to be meaningful**

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

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

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

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

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

376 **3.1.3 Rules for interpreting various name forms**

377 No stipulation.

378 **3.1.4 Uniqueness of names**

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

387 The e-Science CA will make reasonable attempts to ensure that a DN is
388 not reused. If a person requests a certificate with the same DN as an existing
389 certificate (regardless of the status of this certificate) and the request is not
390 a renewal, the RA Operator will consult the original Personal Information
391 to ensure that the Subscriber is the same as the person who was identified
392 in the original certificate.

393 **3.1.5 Name claim dispute resolution procedure**

394 No stipulation.

395 **3.1.6 Recognition, authentication and role of trade-** 396 **marks**

397 No stipulation.

398 **3.1.7 Method to prove possession of private key**

399 No stipulation.

400 **3.1.8 Authentication of organisation identity**

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

404 3.1.9 Authentication of individual identity

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

407 In either case the Subscriber selects which RA is to carry out the identi-
408 fication process.

Person	The Subscriber goes to the selected RA Operator bringing acceptable Personal Information. The RA will take a photo copy of this data, and keep it for auditing purposes (see section B.1).
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).

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

411 3.2 Routine Re-key

412 No stipulation.

413 3.3 Re-key After Revocation

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

416 3.4 Revocation Request

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

421 Authenticated certificate revocation requests may be made by

- 422 • The RA using:
 - 423 – Signed Email to the CA Manager;
 - 424 – Other secure method, as specified in the RA Operator’s procedure.
- 425 • The Subscriber by:
 - 426 – Mailing the CA manager directly by Signed Email.

Chapter 4

OPERATIONAL REQUIREMENTS

4.1 Certificate Application

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

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

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

4.2 Certificate Issuance

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

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

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

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

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

456 All issued certificates are issued under the CP/CPS valid at the time of
457 issuance.

458 **4.3 Certificate Acceptance**

459 No stipulation.

460 **4.4 Certificate Suspension and Revocation**

461 **4.4.1 Circumstances for revocation**

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

- 465 • The CA is informed that the Subscriber has ceased to be a member of
466 or associated with a UK e-Science program or activity;
- 467 • the Subscriber's private key is lost or suspected to be compromised;
- 468 • the information in the Subscriber's certificate is wrong or inaccurate,
469 or suspected to be wrong or inaccurate;
- 470 • the Subscriber violates his/her obligations.

471 **4.4.2 Who can request revocation**

472 A certificate revocation can be requested by:

- 473 • The Registration Authority which authenticated the holder of the cer-
474 tificate;

- 475 • the holder of the certificate;
- 476 • any person presenting proof of knowledge that the Subscriber's private
- 477 key has been compromised or that the Subscriber's data have changed.

478 **4.4.3 Procedure for revocation request**

479 A revocation request is accepted if:

- 480 • The revocation request is signed with the key corresponding to certifi-
- 481 cate whose revocation is requested; or,
- 482 • The revocation request is signed by the RA who originally approved
- 483 the certificate request.

484 Any other revocation request is accepted only if the entity requesting the

485 revocation is properly authenticated.

486 **4.4.4 Revocation request grace period**

487 If the Subscriber discovers that his/her private key is compromised, (s)he

488 must request revocation:

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

493 The Subscriber should request revocation within one working day if any of

494 the other circumstances for revocation are fulfilled.

495 The revocation will take place within one working day of the CA deter-

496 mining the need for revocation.

497 **4.4.5 Circumstances for suspension**

498 The CA does not offer suspension services.

499 **4.4.6 Who can request suspension**

500 No stipulation.

501 **4.4.7 Procedure for suspension request**

502 No stipulation.

503 **4.4.8 Limits on suspension period**

504 No stipulation.

505 **4.4.9 CRL issuance frequency**

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

508 **4.4.10 CRL checking requirements**

509 No stipulation.

510 **4.4.11 On-line revocation/status checking availability**

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

512 **4.4.12 On-line revocation checking requirements**

513 No stipulation.

514 **4.4.13 Other forms of revocation advertisements avail-**
515 **able**

516 No stipulation.

517 **4.4.14 Checking requirements for other forms of revo-**
518 **cation advertisements**

519 No stipulation.

520 **4.4.15 Special requirements re key compromise**

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

525 **4.5 Security Audit Procedures**

526 **4.5.1 Types of event recorded**

527 The following events are recorded:

- 528 • certification requests;
- 529 • issued certificates;
- 530 • requests for revocation;
- 531 • issued CRLs;
- 532 • login/logout/reboot of the signing machine.

533 **4.5.2 Frequency of processing log**

534 No stipulation.

535 **4.5.3 Retention period for audit log**

536 The minimum retention period is 3 years.

537 **4.5.4 Protection of audit log**

538 No stipulation.

539 **4.5.5 Audit log backup procedures**

540 No stipulation.

541 4.5.6 Audit collection system (internal vs external)

542 No stipulation.

543 4.5.7 Notification to event-causing subject

544 No stipulation.

545 4.5.8 Vulnerability assessments

546 No stipulation.

547 4.6 Records Archival**548 4.6.1 Types of event recorded**

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

- 550 • certification requests;
- 551 • issued certificates;
- 552 • requests for revocation;
- 553 • issued CRLs;
- 554 • all e-mail messages received by the CA (not the confirmation messages
555 sent to the Subscribers);
- 556 • all e-mail messages sent by the CA;
- 557 • all documents appointing CA and RA Staff.

558 Each RA must log the following:

- 559 • for each approved request, how it was approved;
- 560 • for each rejected request, why it was rejected;
- 561 • for each approved revocation request, the reason for revocation;
- 562 • for each rejected revocation request, the reason for revocation and the
563 reason the request was rejected.

564 **4.6.2 Retention period for archive**

565 The minimum retention period is 3 years.

566 **4.6.3 Protection of archive**

567 No stipulation.

568 **4.6.4 Archive backup procedures**

569 No stipulation.

570 **4.6.5 Requirements for time-stamping of records**

571 No stipulation.

572 **4.6.6 Archive collection system (internal or external)**

573 No stipulation.

574 **4.6.7 Procedures to obtain and verify archive information**
575

576 No stipulation.

577 **4.7 Key Changeover**

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

582 **4.8 Compromise and Disaster Recovery**

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

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

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

591 **4.8.1 Computing resources, software, and/or data are** 592 **corrupted**

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

594 **4.8.2 Entity public key is revoked**

595 No stipulation.

596 **4.8.3 Entity key is compromised**

597 No stipulation.

598 **4.8.4 Secure facility after a natural or other type of** 599 **disaster**

600 No stipulation.

601 **4.9 CA Termination**

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

- 603 • inform the Registration Authorities, Subscribers, Relying Parties, and
604 cross-certifying CAs of which the CA is aware;
- 605 • make information of its termination widely available;
- 606 • stop issuing certificates.

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

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

617 Chapter 5

618 PHYSICAL, PROCEDURAL, 619 AND PERSONNEL 620 SECURITY CONTROLS

621 5.1 Physical Controls

622 5.1.1 Site location and construction

623 No stipulation.

624 5.1.2 Physical access

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

628 5.1.3 Power and air conditioning

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

631 The signing machine is switched off between signing operations. The machine
632 operates in an air conditioned environment.

633 **5.1.4 Water exposures**

634 No stipulation.

635 **5.1.5 Fire prevention and protection**

636 No stipulation.

637 **5.1.6 Media storage**

638 No stipulation.

639 **5.1.7 Waste disposal**

640 No stipulation.

641 **5.1.8 Off-site backup**

642 No stipulation.

643 **5.2 Procedural Controls**

644 **5.2.1 Trusted roles**

645 No stipulation.

646 **5.2.2 Number of persons required per task**

647 No stipulation.

648 **5.2.3 Identification and authentication for each role**

649 No stipulation.

650 5.3 Personnel Controls

651 5.3.1 Background, qualifications, experience, and clear- 652 ance requirements

- 653 • The CA Manager must be a paid employee of CCLRC and shall be
654 appointed in writing by the CCLRC Director of e-Science who may at
655 his/her discretion revoke the appointment with no prior notice given.

- 656 • The CA Operators must be paid employees of CCLRC and will be
657 appointed by the CA Manager.

- 658 • The RA Manager must be a paid employee of the Physical Organisa-
659 tion hosting that Registration Authority and must be appointed by an
660 Authority responsible for a Department within that physical organisa-
661 tion. The RA Manager must be a member of that Department. The
662 OU field of the RA Operator's certificate identifies the Physical Organ-
663 isation, and the L field identifies the Department where the Manager is
664 appointed. The Authority will make a declaration to the CA Manager
665 in writing on the organisation's headed note paper. The information
666 that must be contained in this letter is defined by the CA Manager.

- 667 • The RA Operator must be a paid employee of the site hosting that
668 Registration Authority and will be appointed by the RA Manager con-
669 cerned. The RA Manager will make a declaration to the CA Manager
670 in writing on the organisation's headed note paper. If the RA Opera-
671 tor is appointed in a different department from the RA Manager then
672 the letter must be countersigned by an authority for the department in
673 which the Operator is appointed. The information that must be con-
674 tained in this letter is defined by the CA Manager. RA Operators must
675 have certificates and must adhere also to the Subscribers' Obligations.

- 676 • An RA Manager may appoint himself/herself as an RA Operator.

- 677 • An RA Manager may appoint any number of RA Operators.

678 5.3.2 Background check procedures

679 No stipulation.

680 **5.3.3 Training requirements**

681 No stipulation.

682 **5.3.4 Retraining frequency and requirements**

683 No stipulation.

684 **5.3.5 Job rotation frequency and sequence**

685 No stipulation.

686 **5.3.6 Sanctions for unauthorized actions**

687 In the event of unauthorised actions, abuse of authority or unauthorised use
688 of entity systems by the CA or RA Operators, the CA manager may revoke
689 the privileges concerned.

690 **5.3.7 Contracting personnel requirements**

691 No stipulation.

692 **5.3.8 Documentation supplied to personnel**

- 693 • It is the responsibility of the CA Manager to provide the CA Operators
694 with a copy of the “e-Science CA Operator’s Procedure”.
- 695 • It is the responsibility of the CA Manager to provide the RA Manager
696 with a copy of the “e-Science RA Manager’s Procedure”.
- 697 • It is the responsibility of the RA Manager to provide the RA Operator
698 with a copy of the “e-Science RA Operator’s Procedure”.

699 Chapter 6

700 TECHNICAL SECURITY 701 CONTROLS

702 6.1 Key Pair Generation and Installation

703 6.1.1 Key pair generation

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

706 6.1.2 Private key delivery to entity

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

709 6.1.3 Public key delivery to certificate issuer

710 Subscribers' public keys are delivered to the issuing CA by the HTTPS pro-
711 tocol via the CA's web interface.

712 6.1.4 CA public key delivery to subscribers

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

715 **6.1.5 Key sizes**

716 Keys of length less than 1024 bits are not accepted. The CA key is of length
717 2048 bits.

718 **6.1.6 Public key parameters generation**

719 No stipulation.

720 **6.1.7 Parameter quality checking**

721 No stipulation.

722 **6.1.8 Hardware/software key generation**

723 No stipulation.

724 **6.1.9 Key usage purposes (as per X.509 v3 key usage 725 field)**

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

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

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

731 **6.2 Private Key Protection**

732 **6.2.1 Standards for cryptographic module**

733 No stipulation.

734 **6.2.2 Private key (n out of m) multi-person control**

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

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

739 **6.2.3 Private key escrow**

740 Private keys must not be escrowed.

741 **6.2.4 Private key backup**

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

746 **6.2.5 Private key archival**

747 No stipulation.

748 **6.2.6 Private key entry into cryptographic module**

749 No stipulation.

750 **6.2.7 Method of activating private key**

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

754 **6.2.8 Method of deactivating private key**

755 No stipulation.

756 **6.2.9 Method of destroying private key**

757 No stipulation.

758 **6.3 Other Aspects of Key Pair Management**

759 **6.3.1 Public key archival**

760 The CA archives all issued certificates.

761 **6.3.2 Usage periods for the public and private keys**

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

764 **6.4 Activation Data**

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

766 **6.4.1 Activation data generation and installation**

767 No stipulation.

768 **6.4.2 Activation data protection**

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

773 **6.4.3 Other aspects of activation data**

774 No stipulation.

775 **6.5 Computer Security Controls**

776 **6.5.1 Specific computer security technical requirements**

777 The CA server includes the following functionality:

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

782 **6.5.2 Computer security rating**

783 No stipulation.

784 **6.6 Life-Cycle Technical Controls**

785 **6.6.1 System development controls**

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

788 **6.6.2 Security management controls**

789 No stipulation.

790 **6.6.3 Life cycle security ratings**

791 No stipulation.

792 **6.7 Network Security Controls**

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

796 **6.8 Cryptographic Module Engineering Con-** 797 **trols**

798 No stipulation.

799 Chapter 7

800 CERTIFICATE AND CRL 801 PROFILES

802 7.1 Certificate Profile

803 7.1.1 Version number

804 X.509.v3

805 7.1.2 Certificate extensions

806 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]
Signature Algorithm		sha1WithRSAEncryption

807 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 Distribution Points	http://ca.grid-support.ac.uk/cgi-bin/importCRL
Netscape Cert Type	SSL CA, S/MIME CA
Signature Algorithm	sha1WithRSAEncryption

808 7.1.3 Algorithm object identifiers

809 No stipulation.

810 7.1.4 Name forms

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

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

814 Issuer as seen with OpenSSL version 0.9.7 or later:

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

817 Subject: The subject field contains the Distinguished Name of the entity
818 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

819 **7.1.5 Name constraints**

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

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

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

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

- 829 • the name of the service,
- 830 • the default port number,
- 831 • a short description of the service,
- 832 • a reference URI.

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

834 **7.1.6 Certificate policy Object Identifier**

835 No stipulation.

836 **7.1.7 Usage of Policy Constraints extensions**

837 No stipulation.

838 **7.1.8 Policy qualifier syntax and semantics**

839 No stipulation.

840 **7.1.9 Processing semantics for the critical certificate**
841 **policy**

842 No stipulation.

843 **7.2 CRL Profile**

844 **7.2.1 Version number**

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

847 **7.2.2 CRL and CRL Entry Extensions**

848 No stipulation.

849 Chapter 8

850 SPECIFICATION 851 ADMINISTRATION

852 8.1 Specification Change Procedures

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

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

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

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

866 *Security updates:* changes that affect the security, e.g. changes to the minimal
867 requirements for verifying requests, or changing the key sizes. These changes
868 will be announced at least 30 days in advance on the CA web site, and to
869 appropriate mailing lists, including the EU Grid PMA mailing list. However,
870 urgent security fixes may be carried out without advance warning and then
871 documented in the CPS. These will be announced in the same manner.

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

874 web site and appropriate mailing lists.

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

877 **8.2 Publication and Notification Policies**

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

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

884 **8.3 CPS Approval Procedures**

885 No stipulation.

886 Appendix A

887 Revision History

888

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.
1.2	1.6	15 May 2005	Documented CA upgrade, Data protection act, and some codifications of existing practice.

889

⁸⁹⁰ The OID in the table is the final two digits of the actual OID, as defined in
⁸⁹¹ section 1.2.

892 Appendix B

893 Compliance with Laws and 894 Regulations

895 The UK e-Science CA operates under UK Law.

896 In the case an RA Operator or CA Operator cannot complete his or her
897 operations without violating rules set forth in this Appendix, the Operator
898 must not complete the operation and must notify the CA Manager, and, if
899 applicable, his or her RA Manager.

900 B.1 The Data Protection Act

901 The Data Protection Act 1998 (DPA) [DPA00].

902 B.1.1 Definitions

- 903 • The *data controller* is the CA Manager, the person mentioned in 1.4.2.
- 904 • The *data processor* is any RA Manager or Operator.
- 905 • The *data subject* is a Subscriber requesting a certificate, or an RA
906 Operator or a CA Operator being appointed as such by the CA.
- 907 • *Data* is to be understood as defined in DPA section I.1.
- 908 • *Processing Data* is to be understood as defined in DPA section I.1.
- 909 • Throughout this Appendix, *Personal Data* means Data which is Per-
910 sonal Data as defined in DPA section I.1 but which is not *Sensitive*
911 *Personal Data* as defined in DPA section I.2.

- 912 • *Personal Information* is defined in section 1.1.1 of this document. For
913 the purposes of the DPA,
- 914 – the photo id is considered Sensitive Personal Data;
- 915 – all other parts of Personal Information are considered Personal
916 Data.

917 **B.1.2 Preliminaries**

918 The *intent* of Processing Data by the UK e-Science CA is that minimal and
919 adequate Personal Information is stored and Processed in order that the UK
920 e-Science CA may operate according to the policy and practices described
921 in this CP/CPS, including being an internationally approved medium level
922 CA.

923 **B.1.3 Data**

924 The UK e-Science CA stores the following Data:

- 925 1. The CA publishes on its web page, and may publish by other methods,
926 the Subscriber's *certificate* and thus all information contained therein,
927 including the Subscriber's name;
- 928 2. The CA logs and stores all Subscriber and RA interactions with the
929 CA's online service, in order to satisfy the requirements of sections 4.5
930 and 4.6 of this CP/CPS;
- 931 3. The RA Operator Processes Personal Information, and possibly other
932 Data, as described in section B.1.5;
- 933 4. The CA stores authorisation information about the RA Manager and
934 Operators sufficient to convince the CA that the RA Manager and
935 Operators satisfy the conditions of section 5.3.1 and that the CA has the
936 RA Manager's assurance that the RA Operator will operate according
937 to this CP/CPS;
- 938 5. For host and service certificates, it may be necessary to obtain and store
939 Personal Data that proves to the RA Operator's satisfaction that Sub-
940 scriber is responsible system administrator for the resource for which
941 the Subscriber requests a certificate, in accordance with sections 2.1.2,
942 2.1.3, and 3.1.9;

943 6. It may be necessary to obtain and store Personal Data to prove to the
944 RA Operator's satisfaction that the Subscriber is entitled to a certifi-
945 cate from the UK e-Science CA, cf. section 1.3.3.

946 Notwithstanding the above, the Data Processed by the UK e-Science CA is
947 subject to the following restrictions:

- 948 • The UK e-Science CA must not Process or attempt to Process any
949 Sensitive Personal Data *except* the photo id.
- 950 • Personal Data and Sensitive Personal Data must be relevant and ade-
951 quate for the purpose for which it is Processed.
- 952 • The UK e-Science CA must Process Personal Information only as de-
953 fined in this Appendix, and in accordance with the DPA.

954 **B.1.4 Consent**

955 By submitting Data to the online CA ([CAW]), the Subscriber is considered
956 to have given consent that the submitted Data may be Processed by the
957 e-Science CA (there is a notice to this effect on the web page). By present-
958 ing Personal Information to the RA Operator, the Subscriber is deemed to
959 have given consent that this information may be Processed according to the
960 purposes described in this document, and stored according to the procedures
961 described in this document (there is a notice to this effect on the web page).
962 By applying for RA Operator or CA Operator status, the RA Operator or CA
963 Operator is deemed to have consented that the CA can Process the Data as
964 described below (there is a notice to this effect in the template appointment
965 letters provided by the CA).

966 **B.1.5 Processing**

967 The CA permits that Personal Information is Processed as follows:

- 968 1. The CA Operator or RA Operator obtains Personal Information or
969 other Data from the Subscriber or from another Operator relevant and
970 adequate for the purposes described below;
- 971 2. A photocopy of the Personal Information is made for the purposes
972 described below;

- 973 3. The photocopy of Personal Information is subsequently accessed only
974 for the purposes described below;
- 975 4. Subscriber's email address is obtained and used only for the purposes
976 described below;
- 977 5. Relevant and adequate information is Processed to satisfy section 4.5
978 of this CP/CPS in accordance with sections 4.5 and 4.6.

979 **B.1.6 Purpose**

980 The UK e-Science CA Processes Personal Information for the following pur-
981 poses:

- 982 1. Identification of a Subscriber;
- 983 2. Subsequent auditing of the Identification process, for the case where the
984 UK e-Science CA must prove the link from the DN to the Subscriber's
985 real identity;
- 986 3. Release of Personal Information under the circumstances described in
987 section 2.8 and according to the procedures described in the same sec-
988 tion;
- 989 4. To maintain the uniqueness of the DN to the extent described in sec-
990 tion 3.1.4;
- 991 5. For RA and CA Operators, to check to the CA Manager's satisfaction
992 that the RA or CA Operator is duly authorised by appointment letter
993 to operate according to this CP/CPS and that the RA Manager and
994 Operator satisfy the conditions described in section 5.3.1;
- 995 6. Adequate Personal Information is Processed to satisfy the auditing re-
996 quirements set forth in sections 2.7, 4.5 and 4.6 of this CP/CPS;
- 997 7. Email address is used only to notify the Subscriber that:
- 998 • A new certificate has been issued to the Subscriber;
- 999 • A certificate held by the Subscriber is about to expire.

1000 Data may be used for statistical purposes

- 1001 • only with the Data Controller's permission; and

- 1002 • if there is reasonable cause; and
- 1003 • if the published information contain neither Personal Data nor Sensitive
1004 Personal Data, and no Personal Data or Sensitive Personal Data can
1005 be derived from it; and
- 1006 • the Processing associated with and required for statistical purposes are
1007 done in accordance with the DPA section 33.

1008 Any other use of Personal Information is explicitly forbidden.

1009 **B.1.7 Data Release**

1010 Circumstances requiring Processing of Personal Information include, but are
1011 not necessarily limited to, the following cases:

- 1012 1. A CA Manager or Operator is considered to have breached CA Obli-
1013 gations (section 2.1.1);
- 1014 2. An RA Manager or Operator is considered to have breached RA Obli-
1015 gations (section 2.1.2);
- 1016 3. A Subscriber is considered to have breached Subscriber's Obligations
1017 (section 2.1.3);
- 1018 4. Release of information as described in section 2.8, including any release
1019 required by UK law;
- 1020 5. Release of information as required for auditing purposes, including com-
1021 pliance audit as described in section 2.7.

1022 In each case, the UK e-Science CA shall ensure that only the adequate and
1023 relevant information is released and that the information is Processed law-
1024 fully and in accordance with the rules of sections B.1.5 and B.1.6, and in
1025 accordance with the DPA.

1026 **B.1.8 Data Maintenance**

1027 There is no requirement for keeping Personal Information Processed by the
1028 RA up to date, except to the extent required to satisfy the RA Operator
1029 that the information mentioned in 5 and 6 in section B.1.3 is still valid if and
1030 when certificates that required this information prior to their approval are
1031 being renewed.

1032 It is the RA Manager's responsibility to ensure that the Data Processed
1033 by the CA concerning his or her RA or any Manager or Operator associated
1034 with that RA is kept up to date, and inform the CA of any update.

1035 **B.1.9 Data Retention**

1036 Personal Information shall be kept by the UK e-Science CA for as long as is
1037 necessary:

- 1038 1. Personal Information used to obtain a personal certificate with a certain
1039 DN shall be kept for as long as the Subscriber has a valid certificate
1040 with this DN, including renewals of the certificate, and for a period
1041 beyond the expiry or revocation of the latest certificate held by the
1042 Subscriber necessary to satisfy the retention requirements described in
1043 section 4.6;
- 1044 2. Data used to obtain a host or service certificate shall be kept for as
1045 long as the Subscriber is responsible administrator for the resource for
1046 which the certificate was obtained, and for a period beyond the expiry
1047 or revocation of the latest certificate held by the Subscriber, or beyond
1048 the administrator rights being passed on to someone else, necessary to
1049 satisfy the retention requirements described in section 4.6.
- 1050 3. Data used by the CA Manager to authorise RA Managers and Op-
1051 erators must be kept for a period beyond the termination of the RA
1052 necessary to satisfy the requirements described in section 4.6. For the
1053 termination of the CA, the conditions in sections 4.6.2 and 4.9 apply.

1054 It is the responsibility of the RA Manager to ensure that appropriate techni-
1055 cal and organisational measures are taken against unlawful or unauthorised
1056 Processing of Data held by the RA. It is the responsibility of the CA Manager
1057 to ensure that appropriate technical and organisational measures are taken
1058 against unlawful or unauthorised Processing of Data held by the CA.

1059 **B.1.10 Data Termination**

1060 It is the responsibility of the RA Manager to ensure that Personal Information
1061 held and Processed by the RA is adequately destroyed by the end of the
1062 retention period. It is the responsibility of the CA Manager to ensure that
1063 Personal Information held and Processed by the CA is adequately destroyed
1064 by the end of the retention period.

1065 Bibliography

- 1066 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate
1067 policy model. [http://www.gridforum.org/2_SEC/pdf/Draft-](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf)
1068 [GGF-CP-06.pdf](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf), September 2001.
- 1069 [BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform resource
1070 locators. <http://www.rfc-editor.org/rfc/rfc1738.txt>, December
1071 1994.
- 1072 [CAC] CA Certificate Revocation List. [http://ca.grid-](http://ca.grid-support.ac.uk/pub/crl/cacrl.crl)
1073 [support.ac.uk/pub/crl/cacrl.crl](http://ca.grid-support.ac.uk/pub/crl/cacrl.crl) (new, DER) and [http://ca.grid-](http://ca.grid-support.ac.uk/pub/crl/cacrl.pem)
1074 [support.ac.uk/pub/crl/cacrl.pem](http://ca.grid-support.ac.uk/pub/crl/cacrl.pem) (new, PEM).
- 1075 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 1076 [Cec01] R. Cecchini. INFN CA CP/CPS. [http://security.fi.infn.it/CA/-](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf)
1077 [CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 1078 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-
1079 ture Certificate Policy and Certification Practices Framework.
1080 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 1081 [CFS+03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet
1082 x.509 public key infrastructure certificate policy and certification
1083 practices framework. [http://www.ietf.org/internet-drafts/draft-](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt)
1084 [ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 1085 [DPA00] Data protection act 1998. [http://www.legislation.hmso.gov.uk/-](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm)
1086 [acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm), March 2000.
- 1087 [Eur00] EuroPKI Certificate Policy. [http://www.europki.org/ca/root/-](http://www.europki.org/ca/root/cps/en_cp.pdf)
1088 [cps/en_cp.pdf](http://www.europki.org/ca/root/cps/en_cp.pdf), October 2000. Version 1.1.
- 1089 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-
1090 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,
1091 December 1999. Version 1.0.

- 1092 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.
1093 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.
1094 Version 1.1.
- 1095 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.
1096 <http://www.globus.org/security/v2.0/index.html>.
- 1097 [Glob] Globus. Grid security infrastructure for globus toolkit 3.
1098 <http://www.globus.org/security/GSI3/index.html>.
- 1099 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 1100 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String
1101 Representation of Standard Attribute Syntaxes. <http://www.rfc-editor.org/rfc/rfc1778.txt>, March 1995.
1102
- 1103 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public
1104 key infrastructure certificate and certificate revocation list (crl)
1105 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 1106 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 1107 [Moc87] P. Mockapetris. Domain names - concepts and facilities.
1108 <http://www.rfc-editor.org/rfc/rfc1034.txt>, November 1987.
- 1109 [NCS99] National Computational Science Alliance Certificate Pol-
1110 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-
1111 Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/Certificates/AllianceCP9.1.html), June 1999.
- 1112 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-
1113 certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 1114 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight
1115 Directory Access Protocol (v3): Attribute Syntax Definitions.
1116 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.