



UK e-Science Certification Authority
Certificate Policy and Certification Practices
Statement
ChangeLog Version 1.1-1.2-1

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

9 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) 16
 - 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 23
 - 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	24
2.3.2	Fiduciary relationships	24
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	25
2.5.1	Certificate issuance or renewal fees	25
2.5.2	Certificate access fees	25
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	26
2.6.3	Access controls	26
2.6.4	Repositories	26
2.7	Compliance Audit	27
2.7.1	Frequency of entity compliance audit	27
2.7.2	Identity/qualifications of auditor	27
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	28
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	29
2.8.5	Release as part of civil discovery	29
2.8.6	Disclosure upon owner's request	29

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 35
3.3 Re-key After Revocation 35
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	<u>Compliance with Laws and Regulations</u>	69
----------	--	-----------

B.1	<u>The Data Protection Act</u>	69
B.1.1	<u>Definitions</u>	69
B.1.2	<u>Preliminaries</u>	70
B.1.3	<u>Data</u>	70
B.1.4	<u>Consent</u>	71
B.1.5	<u>Processing</u>	71
B.1.6	<u>Purpose</u>	72
B.1.7	<u>Data Release</u>	73
B.1.8	<u>Data Maintenance</u>	74
B.1.9	<u>Data Retention</u>	74
B.1.10	<u>Data Termination</u>	75

Chapter 1

INTRODUCTION

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

1.1 Overview

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

This document was issued on 1 May 2005. An update was issued on 9 May 2005.

THIS DOCUMENT IS THE CHANGELOG VERSION BETWEEN
VERSIONS 1.1 AND 1.2. IT IS NOT A VALID CP/CPS. IT
DOCUMENTS CHANGES BETWEEN THE VERSIONS.

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

1.1.1 General definitions

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.
<u>Personal Information</u>	<u>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.</u>
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 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).

17 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	ChangeLog 1.1-1.2
Document date	01 May 2005
Effective from	15 May 2005 (if approved)

18 See also revision history in Appendix A.

19 Throughout this document “CA” refers to the Issuing Certification Authority;
 20 “UK e-Science CA” or “e-Science CA” refer to the whole authority comprising
 21 the CA and all RAs.

22 **1.3 Community and Applicability**

23 **1.3.1 Certification authorities**

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

26 **1.3.2 Registration authorities**

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

34 **1.3.3 End entities (Subscribers)**

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

37 1.3.4 Applicability

38 Certificates issued are suitable for the following applications:

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

43 In addition, it is permissible to use certificates for email signing. ~~Using certificates~~
44 ~~for encryption is not explicitly prohibited but the CA does not support this~~
45 ~~purpose. Encryption is not a permitted purpose.~~

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

48 1.4 Contact Details

49 1.4.1 Specification administration organisation

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

51 1.4.2 Contact person

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

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

65 **1.4.3 Person determining CPS suitability for the pol-**
66 **icy**

67 The person mentioned in 1.4.2.

68 Chapter 2

69 GENERAL PROVISIONS

70 2.1 Obligations

71 2.1.1 CA obligations

72 The CA must:

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

- 87 • produce a detailed statement of procedure conformant to this CPS and
88 make them available to RA staff.

89 The CA is also an RA. For this purpose, the CA Manager is considered
90 the RA Manager for the CA and must adhere also to the RA Manager's
91 obligations. Each CA Operator, when acting as an RA Operator, must
92 adhere also to RA Operators' obligations.

93 **2.1.2 RA obligations**

94 The RA Manager must:

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

110 The RA Operator must:

- 111 • adhere to all Subscriber's Obligations (2.1.3)
- 112 • accept certification requests from entitled entities;
- 113 • for personal certificates, verify the identity of the Subscriber and keep
114 a log of how each Subscriber was identified;
- 115 • ensure that DN is unique according to section 3.1.4;

- 116 ● for both host and service certificates, verify that the Subscriber is
117 the *responsible system administrator* for the resource identified by the
118 certificate, or authorised by the administrator to apply for a certificate;
- 119 ● check that additional location-specific requirements (if any) are fulfilled
120 (an RA may have more stringent requirements for verifying a request
121 than the minimum requirements set out in this policy document - in
122 that case, the RA's web page should list these requirements);
- 123 ● provide information to the Subscriber on how to properly maintain a
124 certificate and the corresponding private key;
- 125 ● check that the information provided in the certificate request is correct
126 as described in section 3.1.9;
- 127 ● sign Subscriber's request when and only when all conditions for issuing
128 a certificate to the Subscriber are fulfilled;
- 129 ● Request revocation of a Subscriber's certificate when and only when
130 the RA Operator is aware that (1) the circumstances for revocation
131 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

132 2.1.3 Subscriber obligations

133 Subscribers must:

- 134 ● read and adhere to the procedures published in this document;
- 135 ● generate a key pair using a trustworthy method;
- 136 ● for personal certificates, choose a unique DN according to section 3.1.4;
- 137 ● for host and service certificates, apply for certificates only for resources
138 for which they are responsible;
- 139 ● for host and service certificates, use an email address in the request
140 which satisfies the requirement that mail sent to that address will
141 reach the Subscriber;
- 142 ● use the certificate for the permitted purposes only;
- 143 ● authorise the processing and conservation of personal data (as required
144 under the Data Protection Act 1998 [DPA00]);

- 145 ● take every precaution to prevent any loss, disclosure or unauthorised
146 access to or use of the private key associated with the certificate, in-
147 cluding:
 - 148 – (personal certificates) selecting a Strong Pass-phrase;
 - 149 – (personal certificates) protecting the pass-phrase from others;
 - 150 – notifying immediately the e-Science CA and any relying parties if
151 the private key is lost or compromised;
 - 152 – requesting revocation if the Subscriber is no longer entitled to a
153 certificate, or if information in the certificate becomes wrong or
154 inaccurate.

155 **2.1.4 Relying party obligations**

156 A Relying Party should accept the Subscriber's certificate for authentication
157 purposes if:

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

166 The Relying Party must:

- 167 ● use the Subscriber's certificates for the permitted purposes only;
- 168 ● use for authorisation purposes either
 - 169 – the Subscriber's full DN; or
 - 170 – only the common root (/C=UK/O=eScience); or
 - 171 – for host or service certificates, the CN or parts of the CN.

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

174 **2.1.5 Repository obligations**

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

177 **2.2 Liability**

178 **2.2.1 CA liability**

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

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

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

194 **2.2.2 RA liability**

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

199 **2.3 Financial Responsibility**

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

201 **2.3.1 Indemnification by relying parties**

202 No stipulation.

203 **2.3.2 Fiduciary relationships**

204 No stipulation.

205 **2.3.3 Administrative processes**

206 No stipulation.

207 **2.4 Interpretation and Enforcement**

208 **2.4.1 Governing law**

209 Interpretation of this policy is according to UK Law.

210 **2.4.2 Severability, survival, merger, notice**

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

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

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

218 **2.4.3 Dispute resolution procedures**

219 No stipulation.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

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

2.5.2 Certificate access fees

No fees are charged for certificate access.

2.5.3 Revocation or status information access fees

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

2.5.4 Fees for other services such as policy information

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

2.5.5 Refund policy

No stipulation.

2.6 Publication and Repositories

2.6.1 Publication of CA information

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

- The e-Science CA's certificate;
- Certificates issued;
- Certificate Revocation Lists;

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

244 **2.6.2 Frequency of publication**

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

248 **2.6.3 Access controls**

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

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

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

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

263 **2.6.4 Repositories**

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

265 **2.7 Compliance Audit**

266 **2.7.1 Frequency of entity compliance audit**

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

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

272 **2.7.2 Identity/qualifications of auditor**

273 No stipulation.

274 **2.7.3 Auditor's relationship to audited party**

275 An external audit can be performed by any UK government department or
276 UK academic institution.

277 **2.7.4 Topics covered by audit**

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

280 **2.7.5 Actions taken as a result of deficiency**

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

283 **2.7.6 Communication of results**

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

2.8 Confidentiality

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

Additionally, for RA Managers and Operators, personal contact information is kept by the CA (work telephone number, work address).

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

2.8.1 Types of information to be kept confidential

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

2.8.2 Types of information not considered confidential

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

Statistics regarding certificates issuance and revocation contain no Personal Information and is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

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

313 **2.8.4 Release to law enforcement officials**

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

317 **2.8.5 Release as part of civil discovery**

318 No stipulation.

319 **2.8.6 Disclosure upon owner's request**

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

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

329 **2.8.7 Other information release circumstances**

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

332 **2.9 Intellectual Property Rights**

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

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

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

340 This document typeset with L^AT_EX.

341 Chapter 3

342 IDENTIFICATION AND 343 AUTHENTICATION

344 3.1 Initial Registration

345 3.1.1 Types of names

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

349 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.

350
351 Common Names (CNs) must be encoded as `PrintableStrings` ([WCHK97],[HKYR95]).

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

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

354 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

355 that is, Space (blank), decimal digits, lower and upper case US ASCII letters,
 356 left and right round brackets, and hyphen. For host and service certificates,
 357 ~~the character '.' (full stop, or period) is also allowed in the Common Name~~
 358 the following characters are permitted:

359 '0' - '9', 'a' - 'z', 'A' - 'Z', '-', '.'

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

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

367 See also 7.1.4.

368 3.1.2 Need for names to be meaningful

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

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

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

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

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

382 3.1.3 Rules for interpreting various name forms

383 No stipulation.

384 **3.1.4 Uniqueness of names**

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

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

399 **3.1.5 Name claim dispute resolution procedure**

400 No stipulation.

401 **3.1.6 Recognition, authentication and role of trade-** 402 **marks**

403 No stipulation.

404 **3.1.7 Method to prove possession of private key**

405 No stipulation.

406 **3.1.8 Authentication of organisation identity**

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

410 3.1.9 Authentication of individual identity

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

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

Person	The Subscriber goes to the selected RA Operator bringing acceptable photo ID <u>Personal Information</u> . 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).

415 ~~For personal certificates we allow in exceptional cases an “External”~~
416 ~~verification for Subscribers who are not able to follow the above procedure~~
417 ~~for personal certificates: The Subscriber can send an email confirming the~~
418 ~~request to the CA. The request is accepted by the CA if the email is signed~~
419 ~~by a certificate from another CA whose certificates are accepted for this~~
420 ~~purpose by the CA Manager. The list of such CAs will be decided by the~~
421 ~~CA Manager and is available on the CA’s web site [CAW]. In this case, the~~
422 ~~CN of the certificate used to sign the email and the CN of the certificate~~
423 ~~request must be identical. Subscribers should not use this procedure unless~~
424 ~~there is no alternative. Subscribers identified through this procedure will~~
425 ~~have OU=CLRC, L=External as RA identifier in their certificates.~~

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

428 **3.2 Routine Re-key**

429 No stipulation.

430 **3.3 Re-key After Revocation**

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

433 **3.4 Revocation Request**

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

438 Authenticated certificate revocation requests may be made by

- 439 • The RA using:
 - 440 – Signed Email to the CA Manager;
 - 441 – Other secure method, as specified in the RA Operator's procedure.
- 442 • The Subscriber by:
 - 443 – Mailing the CA manager directly by Signed Email.

444 Chapter 4

445 OPERATIONAL 446 REQUIREMENTS

447 4.1 Certificate Application

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

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

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

456 4.2 Certificate Issuance

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

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

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

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

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

473 All issued certificates are issued under the CP/CPS valid at the time of
474 issuance.

475 **4.3 Certificate Acceptance**

476 No stipulation.

477 **4.4 Certificate Suspension and Revocation**

478 **4.4.1 Circumstances for revocation**

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

- 482 • The CA is informed that the Subscriber has ceased to be a member of
483 or associated with a UK e-Science program or activity;
- 484 • the Subscriber's private key is lost or suspected to be compromised;
- 485 • the information in the Subscriber's certificate is wrong or inaccurate,
486 or suspected to be wrong or inaccurate;
- 487 • the Subscriber violates his/her obligations.

488 **4.4.2 Who can request revocation**

489 A certificate revocation can be requested by:

- 490 • The Registration Authority which authenticated the holder of the cer-
491 tificate;

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

495 **4.4.3 Procedure for revocation request**

496 A revocation request is accepted if:

- 497 • The revocation request is signed with the key corresponding to certifi-
- 498 cate whose revocation is requested; or,
- 499 • The revocation request is signed by the RA who originally approved
- 500 the certificate request.

501 Any other revocation request is accepted only if the entity requesting the
502 revocation is properly authenticated.

503 **4.4.4 Revocation request grace period**

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

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

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

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

514 **4.4.5 Circumstances for suspension**

515 The CA does not offer suspension services.

516 **4.4.6 Who can request suspension**

517 No stipulation.

518 **4.4.7 Procedure for suspension request**

519 No stipulation.

520 **4.4.8 Limits on suspension period**

521 No stipulation.

522 **4.4.9 CRL issuance frequency**

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

525 **4.4.10 CRL checking requirements**

526 No stipulation.

527 **4.4.11 On-line revocation/status checking availability**

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

529 **4.4.12 On-line revocation checking requirements**

530 No stipulation.

531 **4.4.13 Other forms of revocation advertisements avail-
532 able**

533 No stipulation.

534 **4.4.14 Checking requirements for other forms of revo-
535 cation advertisements**

536 No stipulation.

537 **4.4.15 Special requirements re key compromise**

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

542 **4.5 Security Audit Procedures**

543 **4.5.1 Types of event recorded**

544 The following events are recorded:

- 545 • certification requests;
- 546 • issued certificates;
- 547 • requests for revocation;
- 548 • issued CRLs;
- 549 • login/logout/reboot of the signing machine.

550 **4.5.2 Frequency of processing log**

551 No stipulation.

552 **4.5.3 Retention period for audit log**

553 The minimum retention period is 3 years.

554 **4.5.4 Protection of audit log**

555 No stipulation.

556 **4.5.5 Audit log backup procedures**

557 No stipulation.

558 **4.5.6 Audit collection system (internal vs external)**

559 No stipulation.

560 **4.5.7 Notification to event-causing subject**

561 No stipulation.

562 **4.5.8 Vulnerability assessments**

563 No stipulation.

564 **4.6 Records Archival**

565 **4.6.1 Types of event recorded**

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

- 567 • certification requests;
- 568 • issued certificates;
- 569 • requests for revocation;
- 570 • issued CRLs;
- 571 • all e-mail messages received by the CA (not the confirmation messages
572 sent to the Subscribers);
- 573 • all e-mail messages sent by the CA;
- 574 • all documents appointing CA and RA Staff.

575 Each RA must log the following:

- 576 • for each approved request, how it was approved;
- 577 • for each rejected request, why it was rejected;
- 578 • for each approved revocation request, the reason for revocation;
- 579 • for each rejected revocation request, the reason for revocation and the
580 reason the request was rejected.

581 **4.6.2 Retention period for archive**

582 The minimum retention period is 3 years.

583 **4.6.3 Protection of archive**

584 No stipulation.

585 **4.6.4 Archive backup procedures**

586 No stipulation.

587 **4.6.5 Requirements for time-stamping of records**

588 No stipulation.

589 **4.6.6 Archive collection system (internal or external)**

590 No stipulation.

591 **4.6.7 Procedures to obtain and verify archive information**
592

593 No stipulation.

594 **4.7 Key Changeover**

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

599 **4.8 Compromise and Disaster Recovery**

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

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

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

608 **4.8.1 Computing resources, software, and/or data are** 609 **corrupted**

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

611 **4.8.2 Entity public key is revoked**

612 No stipulation.

613 **4.8.3 Entity key is compromised**

614 No stipulation.

615 **4.8.4 Secure facility after a natural or other type of** 616 **disaster**

617 No stipulation.

618 **4.9 CA Termination**

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

- 620 • inform the Registration Authorities, Subscribers, Relying Parties, and
621 cross-certifying CAs of which the CA is aware;
- 622 • make information of its termination widely available;
- 623 • stop issuing certificates.

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

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

634 Chapter 5

635 PHYSICAL, PROCEDURAL, 636 AND PERSONNEL 637 SECURITY CONTROLS

638 5.1 Physical Controls

639 5.1.1 Site location and construction

640 No stipulation.

641 5.1.2 Physical access

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

645 5.1.3 Power and air conditioning

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

648 The signing machine is switched off between signing operations. The machine
649 operates in an air conditioned environment.

650 **5.1.4 Water exposures**

651 No stipulation.

652 **5.1.5 Fire prevention and protection**

653 No stipulation.

654 **5.1.6 Media storage**

655 No stipulation.

656 **5.1.7 Waste disposal**

657 No stipulation.

658 **5.1.8 Off-site backup**

659 No stipulation.

660 **5.2 Procedural Controls**

661 **5.2.1 Trusted roles**

662 No stipulation.

663 **5.2.2 Number of persons required per task**

664 No stipulation.

665 **5.2.3 Identification and authentication for each role**

666 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.

697 **5.3.3 Training requirements**

698 No stipulation.

699 **5.3.4 Retraining frequency and requirements**

700 No stipulation.

701 **5.3.5 Job rotation frequency and sequence**

702 No stipulation.

703 **5.3.6 Sanctions for unauthorized actions**

704 In the event of unauthorised actions, abuse of authority or unauthorised use
705 of entity systems by the CA or RA Operators, the CA manager may revoke
706 the privileges concerned.

707 **5.3.7 Contracting personnel requirements**

708 No stipulation.

709 **5.3.8 Documentation supplied to personnel**

- 710 • It is the responsibility of the CA Manager to provide the CA Operators
711 with a copy of the “e-Science CA Operator’s Procedure”.
- 712 • It is the responsibility of the CA Manager to provide the RA Manager
713 with a copy of the “e-Science RA Manager’s Procedure”.
- 714 • It is the responsibility of the RA Manager to provide the RA Operator
715 with a copy of the “e-Science RA Operator’s Procedure”.

716 Chapter 6

717 TECHNICAL SECURITY 718 CONTROLS

719 6.1 Key Pair Generation and Installation

720 6.1.1 Key pair generation

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

723 6.1.2 Private key delivery to entity

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

726 6.1.3 Public key delivery to certificate issuer

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

729 6.1.4 CA public key delivery to subscribers

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

732 **6.1.5 Key sizes**

733 Keys of length less than 1024 bits are not accepted. The CA key is of length
734 2048 bits.

735 **6.1.6 Public key parameters generation**

736 No stipulation.

737 **6.1.7 Parameter quality checking**

738 No stipulation.

739 **6.1.8 Hardware/software key generation**

740 No stipulation.

741 **6.1.9 Key usage purposes (as per X.509 v3 key usage 742 field)**

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

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

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

748 **6.2 Private Key Protection**

749 **6.2.1 Standards for cryptographic module**

750 No stipulation.

751 **6.2.2 Private key (n out of m) multi-person control**

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

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

756 **6.2.3 Private key escrow**

757 Private keys must not be escrowed.

758 **6.2.4 Private key backup**

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

763 **6.2.5 Private key archival**

764 No stipulation.

765 **6.2.6 Private key entry into cryptographic module**

766 No stipulation.

767 **6.2.7 Method of activating private key**

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

771 **6.2.8 Method of deactivating private key**

772 No stipulation.

773 **6.2.9 Method of destroying private key**

774 No stipulation.

775 **6.3 Other Aspects of Key Pair Management**

776 **6.3.1 Public key archival**

777 The CA archives all issued certificates.

778 **6.3.2 Usage periods for the public and private keys**

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

781 **6.4 Activation Data**

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

783 **6.4.1 Activation data generation and installation**

784 No stipulation.

785 **6.4.2 Activation data protection**

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

790 **6.4.3 Other aspects of activation data**

791 No stipulation.

792 **6.5 Computer Security Controls**

793 **6.5.1 Specific computer security technical requirements**

794 The CA server includes the following functionality:

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

799 **6.5.2 Computer security rating**

800 No stipulation.

801 **6.6 Life-Cycle Technical Controls**

802 **6.6.1 System development controls**

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

805 **6.6.2 Security management controls**

806 No stipulation.

807 **6.6.3 Life cycle security ratings**

808 No stipulation.

809 **6.7 Network Security Controls**

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

813 **6.8 Cryptographic Module Engineering Con-** 814 **trols**

815 No stipulation.

816 Chapter 7

817 CERTIFICATE AND CRL 818 PROFILES

819 7.1 Certificate Profile

820 7.1.1 Version number

821 X.509.v3

822 7.1.2 Certificate extensions

823 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	https://ca-renew.grid-support.ac.uk/renew.html
Signature Algorithm		sha1WithRSAEncryption

824 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
Signature Algorithm		sha1WithRSAEncryption

825 7.1.3 Algorithm object identifiers

826 No stipulation.

827 7.1.4 Name forms

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

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

831 Issuer as seen with OpenSSL version 0.9.7 or later:

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

834 Subject: The subject field contains the Distinguished Name of the entity
835 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

836 7.1.5 Name constraints

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

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

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

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

- 846 • the name of the service,
- 847 • the default port number,
- 848 • a short description of the service,
- 849 • a reference URI.

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

851 7.1.6 Certificate policy Object Identifier

852 No stipulation.

853 7.1.7 Usage of Policy Constraints extensions

854 No stipulation.

855 **7.1.8 Policy qualifier syntax and semantics**

856 No stipulation.

857 **7.1.9 Processing semantics for the critical certificate**
858 **policy**

859 No stipulation.

860 **7.2 CRL Profile**

861 **7.2.1 Version number**

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

864 **7.2.2 CRL and CRL Entry Extensions**

865 No stipulation.

866 Chapter 8

867 SPECIFICATION 868 ADMINISTRATION

869 8.1 Specification Change Procedures

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

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

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

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

883 *Security updates:* changes that affect the security, e.g. changes to the minimal
884 requirements for verifying requests, or changing the key sizes. These changes
885 will be announced at least 30 days in advance on the CA web site, and to
886 appropriate mailing lists, including the ~~DataGrid-CA~~ EU Grid PMA mailing
887 list. However, urgent security fixes may be carried out without advance
888 warning and then documented in the CPS. These will be announced in the
889 same manner.

890 *Policy updates:* e.g. changes to the namespace, or introducing subordinate

891 CAs. A proposal will be announced at least 30 days in advance on the CA
892 web site and appropriate mailing lists.

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

895 **8.2 Publication and Notification Policies**

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

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

902 **8.3 CPS Approval Procedures**

903 No stipulation.

904 **Appendix A**

905 **Revision History**

906

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 up several parts, including Applicability, personal information stored, etc.
1.0	1.4	30 October 2003	
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.

907

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

910 Appendix B

911 Compliance with Laws and 912 Regulations

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

914 In the case an RA Operator or CA Operator cannot complete his or her
915 operations without violating rules set forth in this Appendix, the Operator
916 must not complete the operation and must notify the CA Manager, and, if
917 applicable, his or her RA Manager.

918 B.1 The Data Protection Act

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

920 B.1.1 Definitions

- 921 • The *data controller* is the CA Manager, the person mentioned in 1.4.2.
- 922 • The *data processor* is any RA Manager or Operator.
- 923 • The *data subject* is a Subscriber requesting a certificate, or an RA
924 Operator or a CA Operator being appointed as such by the CA.
- 925 • *Data* is to be understood as defined in DPA section I.1.
- 926 • *Processing Data* is to be understood as defined in DPA section I.1.

- 927 • Throughout this Appendix, *Personal Data* means Data which is Personal
928 Data as defined in DPA section I.1 but which is not *Sensitive Personal Data*
929 as defined in DPA section I.2.

- 930 • *Personal Information* is defined in section 1.1.1 of this document. For
931 the purposes of the DPA,
 - 932 – the photo id is considered Sensitive Personal Data;
 - 933 – all other parts of Personal Information are considered Personal
934 Data.

935 **B.1.2 Preliminaries**

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

941 **B.1.3 Data**

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

- 943 1. The CA publishes on its web page, and may publish by other methods,
944 the Subscriber's *certificate* and thus all information contained therein,
945 including the Subscriber's name;

- 946 2. The CA logs and stores all Subscriber and RA interactions with the
947 CA's online service, in order to satisfy the requirements of sections 4.5
948 and 4.6 of this CP/CPS;

- 949 3. The RA Operator Processes Personal Information, and possibly other
950 Data, as described in section B.1.5;

- 951 4. The CA stores authorisation information about the RA Manager and
952 Operators sufficient to convince the CA that the RA Manager and
953 Operators satisfy the conditions of section 5.3.1 and that the CA has the
954 RA Manager's assurance that the RA Operator will operate according
955 to this CP/CPS;

956 5. For host and service certificates, it may be necessary to obtain and
957 store Personal Data that proves to the RA Operator's satisfaction
958 that Subscriber is responsible system administrator for the resource for
959 which the Subscriber requests a certificate, in accordance with sections
960 2.1.2, 2.1.3, and 3.1.9;

961 6. It may be necessary to obtain and store Personal Data to prove to
962 the RA Operator's satisfaction that the Subscriber is entitled to a
963 certificate from the UK e-Science CA, cf. section 1.3.3.

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

- 966 • The UK e-Science CA must not Process or attempt to Process any
967 Sensitive Personal Data *except* the photo id.
- 968 • Personal Data and Sensitive Personal Data must be relevant and adequate
969 for the purpose for which it is Processed.
- 970 • The UK e-Science CA must Process Personal Information only as defined
971 in this Appendix, and in accordance with the DPA.

972 **B.1.4** Consent

973 By submitting Data to the online CA ([CAW]), the Subscriber is considered
974 to have given consent that the submitted Data may be Processed by the
975 e-Science CA (there is a notice to this effect on the web page). By presenting
976 Personal Information to the RA Operator, the Subscriber is deemed to
977 have given consent that this information may be Processed according to the
978 purposes described in this document, and stored according to the procedures
979 described in this document (there is a notice to this effect on the web page).
980 By applying for RA Operator or CA Operator status, the RA Operator or CA
981 Operator is deemed to have consented that the CA can Process the Data as
982 described below (there is a notice to this effect in the template appointment
983 letters provided by the CA).

984 **B.1.5** Processing

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

- 986 1. The CA Operator or RA Operator obtains Personal Information or
987 other Data from the Subscriber or from another Operator relevant and
988 adequate for the purposes described below;
- 989 2. A photocopy of the Personal Information is made for the purposes
990 described below;
- 991 3. The photocopy of Personal Information is subsequently accessed only
992 for the purposes described below;
- 993 4. Subscriber's email address is obtained and used only for the purposes
994 described below;
- 995 5. Relevant and adequate information is Processed to satisfy section 4.5
996 of this CP/CPS in accordance with sections 4.5 and 4.6.

997 **B.1.6 Purpose**

998 The UK e-Science CA Processes Personal Information for the following purposes:

- 999 1. Identification of a Subscriber;
- 1000 2. Subsequent auditing of the Identification process, for the case where the
1001 UK e-Science CA must prove the link from the DN to the Subscriber's
1002 real identity;
- 1003 3. Release of Personal Information under the circumstances described in
1004 section 2.8 and according to the procedures described in the same
1005 section;
- 1006 4. To maintain the uniqueness of the DN to the extent described in
1007 section 3.1.4;
- 1008 5. For RA and CA Operators, to check to the CA Manager's satisfaction
1009 that the RA or CA Operator is duly authorised by appointment letter
1010 to operate according to this CP/CPS and that the RA Manager and
1011 Operator satisfy the conditions described in section 5.3.1;
- 1012 6. Adequate Personal Information is Processed to satisfy the auditing
1013 requirements set forth in sections 2.7, 4.5 and 4.6 of this CP/CPS;
- 1014 7. Email address is used only to notify the Subscriber that:
1015
 - A new certificate has been issued to the Subscriber;

- 1016 • A certificate held by the Subscriber is about to expire.

1017 Data may be used for statistical purposes

- 1018 • only with the Data Controller's permission; and
- 1019 • if there is reasonable cause; and
- 1020 • if the published information contain neither Personal Data nor Sensitive
1021 Personal Data, and no Personal Data or Sensitive Personal Data can
1022 be derived from it; and
- 1023 • the Processing associated with and required for statistical purposes are
1024 done in accordance with the DPA section 33.

1025 Any other use of Personal Information is explicitly forbidden.

1026 **B.1.7 Data Release**

1027 Circumstances requiring Processing of Personal Information include, but are
1028 not necessarily limited to, the following cases:

- 1029 1. A CA Manager or Operator is considered to have breached CA Obligations
1030 (section 2.1.1);
- 1031 2. An RA Manager or Operator is considered to have breached RA Obligations
1032 (section 2.1.2);
- 1033 3. A Subscriber is considered to have breached Subscriber's Obligations
1034 (section 2.1.3);
- 1035 4. Release of information as described in section 2.8, including any release
1036 required by UK law;
- 1037 5. Release of information as required for auditing purposes, including
1038 compliance audit as described in section 2.7.

1039 In each case, the UK e-Science CA shall ensure that only the adequate
1040 and relevant information is released and that the information is Processed
1041 lawfully and in accordance with the rules of sections B.1.5 and B.1.6, and in
1042 accordance with the DPA.

1043 **B.1.8 Data Maintenance**

1044 There is no requirement for keeping Personal Information Processed by the
1045 RA up to date, except to the extent required to satisfy the RA Operator
1046 that the information mentioned in 5 and 6 in section B.1.3 is still valid if and
1047 when certificates that required this information prior to their approval are
1048 being renewed.

1049 It is the RA Manager's responsibility to ensure that the Data Processed
1050 by the CA concerning his or her RA or any Manager or Operator associated
1051 with that RA is kept up to date, and inform the CA of any update.

1052 **B.1.9 Data Retention**

1053 Personal Information shall be kept by the UK e-Science CA for as long as is
1054 necessary:

- 1055 1. Personal Information used to obtain a personal certificate with a certain
1056 DN shall be kept for as long as the Subscriber has a valid certificate
1057 with this DN, including renewals of the certificate, and for a period
1058 beyond the expiry or revocation of the latest certificate held by the
1059 Subscriber necessary to satisfy the retention requirements described in
1060 section 4.6;
- 1061 2. Data used to obtain a host or service certificate shall be kept for as
1062 long as the Subscriber is responsible administrator for the resource for
1063 which the certificate was obtained, and for a period beyond the expiry
1064 or revocation of the latest certificate held by the Subscriber, or beyond
1065 the administrator rights being passed on to someone else, necessary to
1066 satisfy the retention requirements described in section 4.6.
- 1067 3. Data used by the CA Manager to authorise RA Managers and Operators
1068 must be kept for a period beyond the termination of the RA necessary
1069 to satisfy the requirements described in section 4.6. For the termination
1070 of the CA, the conditions in sections 4.6.2 and 4.9 apply.

1071 It is the responsibility of the RA Manager to ensure that appropriate technical
1072 and organisational measures are taken against unlawful or unauthorised Processing
1073 of Data held by the RA. It is the responsibility of the CA Manager to ensure
1074 that appropriate technical and organisational measures are taken against
1075 unlawful or unauthorised Processing of Data held by the CA.

1076 **B.1.10 Data Termination**

1077 It is the responsibility of the RA Manager to ensure that Personal Information
1078 held and Processed by the RA is adequately destroyed by the end of the
1079 retention period. It is the responsibility of the CA Manager to ensure that
1080 Personal Information held and Processed by the CA is adequately destroyed
1081 by the end of the retention period.

1082 Bibliography

- 1083 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate
1084 policy model. [http://www.gridforum.org/2_SEC/pdf/Draft-](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf)
1085 [GGF-CP-06.pdf](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf), September 2001.
- 1086 [BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform resource
1087 locators. <http://www.rfc-editor.org/rfc/rfc1738.txt>, December
1088 1994.
- 1089 [CAC] CA Certificate Revocation List. [http://ca.grid-support.ac.uk/-](http://ca.grid-support.ac.uk/cgi-bin/importCRL)
1090 [cgi-bin/importCRL](http://ca.grid-support.ac.uk/cgi-bin/importCRL).
- 1091 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 1092 [Cec01] R. Cecchini. INFN CA CP/CPS. [http://security.fi.infn.it/CA/-](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf)
1093 [CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 1094 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-
1095 ture Certificate Policy and Certification Practices Framework.
1096 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 1097 [CFS⁺03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet
1098 x.509 public key infrastructure certificate policy and certification
1099 practices framework. [http://www.ietf.org/internet-drafts/draft-](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt)
1100 [ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 1101 [DPA00] Data protection act 1998. [http://www.legislation.hmso.gov.uk/-](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm)
1102 [acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm), March 2000.
- 1103 [Eur00] EuroPKI Certificate Policy. [http://www.europki.org/ca/root/-](http://www.europki.org/ca/root/cps/en_cp.pdf)
1104 [cps/en_cp.pdf](http://www.europki.org/ca/root/cps/en_cp.pdf), October 2000. Version 1.1.
- 1105 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-
1106 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,
1107 December 1999. Version 1.0.

- 1108 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.
1109 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.
1110 Version 1.1.
- 1111 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.
1112 <http://www.globus.org/security/v2.0/index.html>.
- 1113 [Glob] Globus. Grid security infrastructure for globus toolkit 3.
1114 <http://www.globus.org/security/GSI3/index.html>.
- 1115 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 1116 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String
1117 Representation of Standard Attribute Syntaxes. <http://www.rfc-editor.org/rfc/rfc1778.txt>, March 1995.
1118
- 1119 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public
1120 key infrastructure certificate and certificate revocation list (crl)
1121 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 1122 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 1123 [Moc87] P. Mockapetris. Domain names - concepts and facilities.
1124 <http://www.rfc-editor.org/rfc/rfc1034.txt>, November 1987.
- 1125 [NCS99] National Computational Science Alliance Certificate Pol-
1126 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-
1127 Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/Certificates/AllianceCP9.1.html), June 1999.
- 1128 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-
1129 certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 1130 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight
1131 Directory Access Protocol (v3): Attribute Syntax Definitions.
1132 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.