

UK e-Science Certification Authority
Certificate Policy and Certification Practices
Statement
Version 1.4
1.3.6.1.4.1.11439.1.1.1.1.8

Jens G Jensen

Science and Technology Facilities Council

Rutherford Appleton Laboratory

26 Nov 2007

Contents

- 1 INTRODUCTION 11**
 - 1.1 Overview 11
 - 1.1.1 General definitions 11
 - 1.2 Identification 16
 - 1.3 Community and Applicability 16
 - 1.3.1 Certification authorities 16
 - 1.3.2 Registration authorities 17
 - 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 18
 - 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 23
 - 2.1.5 Repository obligations 23
 - 2.2 Liability 24
 - 2.2.1 CA liability 24
 - 2.2.2 RA liability 24
 - 2.3 Financial Responsibility 24

2.3.1	Indemnification by relying parties	24
2.3.2	Fiduciary relationships	24
2.3.3	Administrative processes	25
2.4	Interpretation and Enforcement	25
2.4.1	Governing law	25
2.4.2	Severability, survival, merger, notice	25
2.4.3	Dispute resolution procedures	25
2.5	Fees	26
2.5.1	Certificate issuance or renewal fees	26
2.5.2	Certificate access fees	26
2.5.3	Revocation or status information access fees	26
2.5.4	Fees for other services such as policy information	26
2.5.5	Refund policy	26
2.6	Publication and Repositories	26
2.6.1	Publication of CA information	26
2.6.2	Frequency of publication	27
2.6.3	Access controls	27
2.6.4	Repositories	27
2.7	Compliance Audit	28
2.7.1	Frequency of entity compliance audit	28
2.7.2	Identity/qualifications of auditor	28
2.7.3	Auditor's relationship to audited party	28
2.7.4	Topics covered by audit	28
2.7.5	Actions taken as a result of deficiency	28
2.7.6	Communication of results	28
2.8	Confidentiality	29
2.8.1	Types of information to be kept confidential	29
2.8.2	Types of information not considered confidential	29
2.8.3	Disclosure of certificate revocation/suspension information	29
2.8.4	Release to law enforcement officials	29
2.8.5	Release as part of civil discovery	30
2.8.6	Disclosure upon owner's request	30

2.8.7 Other information release circumstances 30
2.9 Intellectual Property Rights 30

3 IDENTIFICATION AND AUTHENTICATION 33

3.1 Initial Registration 33
3.1.1 Types of names 33
3.1.2 Need for names to be meaningful 35
3.1.3 Rules for interpreting various name forms 36
3.1.4 Uniqueness of names 36
3.1.5 Name claim dispute resolution procedure 36
3.1.6 Recognition, authentication and role of trademarks . . 36
3.1.7 Method to prove possession of private key 36
3.1.8 Authentication of organisation identity 37
3.1.9 Authentication of individual identity 37
3.2 Routine Re-key 38
3.3 Re-key After Revocation 38
3.4 Revocation Request 38

4 OPERATIONAL REQUIREMENTS 41

4.1 Certificate Application 41
4.2 Certificate Issuance 42
4.3 Certificate Acceptance 42
4.4 Certificate Suspension and Revocation 42
4.4.1 Circumstances for revocation 42
4.4.2 Who can request revocation 43
4.4.3 Procedure for revocation request 43
4.4.4 Revocation request grace period 44
4.4.5 Circumstances for suspension 44
4.4.6 Who can request suspension 44
4.4.7 Procedure for suspension request 44
4.4.8 Limits on suspension period 44
4.4.9 CRL issuance frequency 44
4.4.10 CRL checking requirements 44
4.4.11 On-line revocation/status checking availability 45

4.4.12	On-line revocation checking requirements	45
4.4.13	Other forms of revocation advertisements available . . .	45
4.4.14	Checking requirements for other forms of revocation advertisements	45
4.4.15	Special requirements re key compromise	45
4.5	Security Audit Procedures	45
4.5.1	Types of event recorded	45
4.5.2	Frequency of processing log	46
4.5.3	Retention period for audit log	46
4.5.4	Protection of audit log	46
4.5.5	Audit log backup procedures	46
4.5.6	Audit collection system (internal vs external)	46
4.5.7	Notification to event-causing subject	46
4.5.8	Vulnerability assessments	46
4.6	Records Archival	46
4.6.1	Types of event recorded	46
4.6.2	Retention period for archive	47
4.6.3	Protection of archive	47
4.6.4	Archive backup procedures	47
4.6.5	Requirements for time-stamping of records	47
4.6.6	Archive collection system (internal or external)	47
4.6.7	Procedures to obtain and verify archive information . . .	48
4.7	Key Changeover	48
4.8	Compromise and Disaster Recovery	48
4.8.1	Computing resources, software, and/or data are cor- rupted	48
4.8.2	Entity public key is revoked	48
4.8.3	Entity key is compromised	48
4.8.4	Secure facility after a natural or other type of disaster .	49
4.9	CA Termination	49
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	51
5.1	Physical Controls	51

5.1.1	Site location and construction	51
5.1.2	Physical access	51
5.1.3	Power and air conditioning	51
5.1.4	Water exposures	52
5.1.5	Fire prevention and protection	52
5.1.6	Media storage	52
5.1.7	Waste disposal	52
5.1.8	Off-site backup	52
5.2	Procedural Controls	52
5.2.1	Trusted roles	52
5.2.2	Number of persons required per task	52
5.2.3	Identification and authentication for each role	52
5.3	Personnel Controls	53
5.3.1	Background, qualifications, experience, and clearance requirements	53
5.3.2	Background check procedures	53
5.3.3	Training requirements	54
5.3.4	Retraining frequency and requirements	54
5.3.5	Job rotation frequency and sequence	54
5.3.6	Sanctions for unauthorized actions	54
5.3.7	Contracting personnel requirements	54
5.3.8	Documentation supplied to personnel	54
6	TECHNICAL SECURITY CONTROLS	55
6.1	Key Pair Generation and Installation	55
6.1.1	Key pair generation	55
6.1.2	Private key delivery to entity	55
6.1.3	Public key delivery to certificate issuer	55
6.1.4	CA public key delivery to subscribers	55
6.1.5	Key sizes	56
6.1.6	Public key parameters generation	56
6.1.7	Parameter quality checking	56
6.1.8	Hardware/software key generation	56

6.1.9	Key usage purposes (as per X.509 v3 key usage field)	56
6.2	Private Key Protection	56
6.2.1	Standards for cryptographic module	58
6.2.2	Private key (n out of m) multi-person control	58
6.2.3	Private key escrow	58
6.2.4	Private key backup	58
6.2.5	Private key archival	59
6.2.6	Private key entry into cryptographic module	59
6.2.7	Method of activating private key	59
6.2.8	Method of deactivating private key	59
6.2.9	Method of destroying private key	59
6.3	Other Aspects of Key Pair Management	59
6.3.1	Public key archival	59
6.3.2	Usage periods for the public and private keys	59
6.4	Activation Data	60
6.4.1	Activation data generation and installation	60
6.4.2	Activation data protection	60
6.4.3	Other aspects of activation data	60
6.5	Computer Security Controls	60
6.5.1	Specific computer security technical requirements	60
6.5.2	Computer security rating	61
6.6	Life-Cycle Technical Controls	61
6.6.1	System development controls	61
6.6.2	Security management controls	61
6.6.3	Life cycle security ratings	61
6.7	Network Security Controls	61
6.8	Cryptographic Module Engineering Controls	61
7	CERTIFICATE AND CRL PROFILES	63
7.1	Certificate Profile	63
7.1.1	Version number	63
7.1.2	Certificate extensions	63
7.1.3	Algorithm object identifiers	65

<i>CONTENTS</i>	9
7.1.4 Name forms	65
7.1.5 Name constraints	67
7.1.6 Certificate policy Object Identifier	68
7.1.7 Usage of Policy Constraints extensions	68
7.1.8 Policy qualifier syntax and semantics	68
7.1.9 Processing semantics for the critical certificate policy .	68
7.2 CRL Profile	68
7.2.1 Version number	68
7.2.2 CRL and CRL Entry Extensions	68
8 SPECIFICATION ADMINISTRATION	69
8.1 Specification Change Procedures	69
8.2 Publication and Notification Policies	70
8.3 CPS Approval Procedures	70
A Revision History	71
B Compliance with Laws and Regulations	75
B.1 The Data Protection Act	75
B.1.1 Definitions	75
B.1.2 Preliminaries	76
B.1.3 Data	76
B.1.4 Consent	77
B.1.5 Processing	77
B.1.6 Purpose	78
B.1.7 Data Release	79
B.1.8 Data Maintenance	79
B.1.9 Data Retention	80
B.1.10 Data Termination	80

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 is the CP/CPS for the UK e-Science CA. The first changelog version of it was issued on 26 Nov 2007, and with a subsequent minor update (fixed a typo) on 03 Dec 2007. Apart from version information and this text, this document is identical to the changelog version with the changes committed.

THIS DOCUMENT IS A VALID CP/CPS AS OF 4 DEC 2007, 11:00 UTC.

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.
NGS	The UK National Grid Service
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.

Robot	A Robot is defined as an independent personal credential, issued to a specific user, which can perform automated client tasks on behalf of the user. Since the private key cannot be passphrase protected (except by exposing the passphrase) and the certificate is not tied to a network identity, the private key must have special protection.
Service	A service a GSI service (see GSI); it is approximately the same as URL <i>scheme</i> (cf. RFC1738), but is usually meaningful only to Globus protocols.
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 sender address is the same as the one in the subject alternative name.
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.
------------	---

1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	Version 1.4
Document date	26 Nov 2007
Effective from	04 Dec 2007
Document OID	1.3.6.1.4.1.11439.1.1.1.1.8

The document OID is `{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) cclrc(11439) 1 escience(1) ca(1) cps(1) 8}`.

See also revision history in Appendix A.

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

1.3 Community and Applicability

1.3.1 Certification authorities

The e-Science CA is a subordinate CA under the e-Science Root CA. It does not issue certificates to subordinate CAs.

27 **1.3.2 Registration authorities**

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

35 **1.3.3 End entities (Subscribers)**

36 The e-Science CA issues certificates for e-Science activities funded by the UK
37 Research Councils. The CA will issue personal, and host, service, and robot
38 certificates.

39 **1.3.4 Applicability**

40 Certificates issued are suitable for the following applications:

- 41 • SSL or GSI client (all certificates);
- 42 • SSL or GSI server (host and service certificates only);
- 43 • GSI service (service certificates only);
- 44 • Generating GSI proxies (all certificates);

45 In addition, it is permissible to use certificates for email signing. Long-term
46 (archival) encryption is not a permitted purpose, but ephemeral encryption
47 is permitted.

48 Notwithstanding the above, using certificates for purposes contrary to
49 applicable law (see section 2.4.1) is explicitly prohibited.

50 **1.4 Contact Details**

51 **1.4.1 Specification administration organisation**

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

53 **1.4.2 Contact person**

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

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

67 **1.4.3 Person determining CPS suitability for the pol-** 68 **icy**

69 The person mentioned in 1.4.2.

70 Chapter 2

71 GENERAL PROVISIONS

72 2.1 Obligations

73 2.1.1 CA obligations

74 The CA must:

- 75 • publish a CP and a CPS, structured according to RFC2527, [CF99];
- 76 • ensure that operations and infrastructure conform to this CP/CPS;
- 77 • issue certificates to entitled Subscribers based on validated requests
78 from Registration Authorities;
- 79 • notify the Subscriber of the issuing of the certificate;
- 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 • identify and publish a list of the robots for which robot certificates are
88 issued (cf. sections 3.1.2 and 7.1.2);

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

91 The CA is also an RA. The CA Manager appoints an RA Manager for
92 the CA who must adhere to the RA Manager's obligations. Each CA Oper-
93 ator, when acting as an RA Operator, must adhere also to RA Operators'
94 obligations.

95 **2.1.2 RA obligations**

96 The RA Manager must:

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

112 The RA Operator must:

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

- 118 • for both host and service certificates, verify that the Subscriber is the
119 *responsible system administrator* for the resource identified by the cer-
120 tificate, or authorised by the administrator to apply for a certificate;
- 121 • for robot certificates, verify that the applicant has satisfied the robot
122 requirements (cf. sections 4.1 and 3.1.2);
- 123 • check that additional location-specific requirements (if any) are fulfilled
124 (an RA may have more stringent requirements for verifying a request
125 than the minimum requirements set out in this policy document - in
126 that case, the RA’s web page should list these requirements);
- 127 • comply with the DPA compliance statement set out in Appendix B.1,
128 and, in particular:
 - 129 – ask the Subscriber only for adequate and relevant information
130 necessary to validate the request according to this CP/CPS and
131 to additional RA-specific requirements, and
 - 132 – process any personal data given by the subscriber (regardless of
133 its adequacy or relevance) according to the DPA compliance state-
134 ment in Appendix B.1;
- 135 • provide information to the Subscriber on how to properly maintain a
136 certificate and the corresponding private key;
- 137 • check that the information provided in the certificate request is correct
138 as described in section 3.1.9;
- 139 • sign Subscriber’s request when and only when all conditions for issuing
140 a certificate to the Subscriber are fulfilled;
- 141 • Request revocation of a Subscriber’s certificate when and only when
142 the RA Operator is aware that (1) the circumstances for revocation
143 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

144 **2.1.3 Subscriber obligations**

145 Subscribers must:

- 146 • adhere to the procedures published in this document;
- 147 • generate a key pair using a trustworthy method;

- 148 ● for personal certificates, choose a unique DN according to section 3.1.4,
149 and supply a valid personal email address;
- 150 ● for host and service certificates, apply for certificates only for resources
151 for which they are responsible;
- 152 ● for host and service certificates, use an email address in the request
153 which satisfies the requirement that mail sent to that address will
154 reach the Subscriber;
- 155 ● for robot certificates, ensure that the requirements for robot certificates
156 are fulfilled (cf. sections 4.1 and 3.1.2);
- 157 ● use the certificate for the permitted purposes only;
- 158 ● authorise the processing and conservation of personal data (as required
159 under the Data Protection Act 1998 [DPA00]);
- 160 ● take every precaution to prevent any loss, disclosure or unauthorised
161 access to or use of the private key associated with the certificate, in-
162 cluding:
 - 163 – (personal certificates) selecting a Strong Pass-phrase;
 - 164 – (personal certificates) protecting the pass-phrase from others;
 - 165 – notifying immediately the e-Science CA and any relying parties if
166 the private key is lost or compromised;
 - 167 – requesting revocation if the Subscriber is no longer entitled to a
168 certificate, or if information in the certificate becomes wrong or
169 inaccurate.
 - 170 – (robot certificates) using a secure key token to protect the private
171 key.

172 It is the Subscriber's obligation to provide to the RA Operator the informa-
173 tion required by the RA Operator to validate the request. This information
174 may depend on the type of request. However, the RA operator must ask
175 only for relevant and adequate information to validate the request (cf. Ap-
176 pendix B.1) and the Subscriber is under no obligation to provide further
177 information.

178 By submitting such information to the RA Operator, the Subscriber shall
179 be considered to have consented that *all* the information may be processed
180 by the CA and RA according to the DPA compliance statements in Ap-
181 pendix B.1.

182 **2.1.4 Relying party obligations**

183 A Relying Party should accept the Subscriber's certificate for authentication
184 purposes if:

- 185 • the Relying Party is familiar with the CA's CP and the CPS under
186 which the certificate was issued before drawing any conclusion on trust
187 of the Subscriber's certificate; and
- 188 • the reliance is reasonable and in good faith in light of all circumstances
189 known to the Relying Party at the time of reliance; and
- 190 • the certificate is used for permitted purposes only; and
- 191 • the Relying Party checked the validity and status of the certificate to
192 their own satisfaction prior to reliance.

193 The Relying Party must:

- 194 • use the Subscriber's certificates for the permitted purposes only;
- 195 • use for authorisation purposes either
 - 196 – the Subscriber's full DN; or
 - 197 – only the common root (*/C=UK/O=eScience/*); or
 - 198 – for host or service certificates, the CN or parts of the CN; or
 - 199 – for robot certificates, the Robot CN (see section 3.1.2 and 7.1.2).

200 In particular, the RP must not rely on either or both of the OU or L
201 for authorisation purposes. The RP must not rely on the presence of,
202 or content of, disambiguation strings for authorisation purposes.

203 **2.1.5 Repository obligations**

204 The e-Science CA will publish on its web server [CAW] according to 4.4.9.

205 **2.2 Liability**

206 **2.2.1 CA liability**

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

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

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

222 **2.2.2 RA liability**

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

227 **2.3 Financial Responsibility**

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

229 **2.3.1 Indemnification by relying parties**

230 No stipulation.

231 **2.3.2 Fiduciary relationships**

232 No stipulation.

233 **2.3.3 Administrative processes**

234 No stipulation.

235 **2.4 Interpretation and Enforcement**

236 **2.4.1 Governing law**

237 This policy is governed by, and is to be construed in accordance with, English
238 law. The English Courts will have exclusive jurisdiction to deal with any
239 dispute which has arisen, or may arise out of, or in connection with, this
240 policy.

241 **2.4.2 Severability, survival, merger, notice**

242 If any part or any provision of this document shall to any extent prove in-
243 valid or unenforceable in law, including the laws of the European Union, the
244 remainder of such provision and all other provisions of this document shall re-
245 main valid and enforceable to the fullest extent permissible by law, and such
246 provision shall be deemed to be omitted from this document to the extent
247 of such invalidity or unenforceability. The remainder of this document shall
248 continue in full force and effect and the e-Science CA, Subscribers, and RPs
249 shall negotiate in good faith to replace the invalid or unenforceable provision
250 with a valid, legal and enforceable provision which has an effect as close as
251 possible to the provision or terms being replaced.

252 In the event that the CA ceases operation, all Subscribers, sponsoring
253 organisations, RAs, and Relying Parties will be promptly notified of the
254 termination.

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

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

259 **2.4.3 Dispute resolution procedures**

260 No stipulation.

261 **2.5 Fees**

262 **2.5.1 Certificate issuance or renewal fees**

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

265 **2.5.2 Certificate access fees**

266 No stipulation.

267 **2.5.3 Revocation or status information access fees**

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

270 **2.5.4 Fees for other services such as policy information**

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

274 **2.5.5 Refund policy**

275 No stipulation.

276 **2.6 Publication and Repositories**

277 **2.6.1 Publication of CA information**

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

- 279 • The e-Science CA's certificate;
- 280 • Certificate Revocation Lists;
- 281 • A copy of the most recent version of this CP/CPS and all previous
282 versions since 0.7;

- 283 • A changelog version of each CP/CPS comparing it to the previous
284 (except 0.7 which was the first public version).
- 285 • Other relevant information.

286 **2.6.2 Frequency of publication**

- 287 • CRLs will be published as described in 4.4.9.
- 288 • This CP/CPS will be published whenever it is updated.

289 **2.6.3 Access controls**

290 The online repository is maintained on best effort basis and is available sub-
291 stantially on a 24 hours per day, 7 days per week basis, subject to reason-
292 able scheduled maintenance. Outside the period 08:00-17:00 (BST) Monday-
293 Friday it may run unattended “at risk”.

294 The e-Science CA does not impose any access control on its CP/CPS, its
295 certificate, or CRLs.

296 The e-Science CA does impose access control on the issued certificates.

297 Furthermore, a valid personal certificate must be used to submit a request
298 for the following types of certificates:

- 299 • a rekey of the same certificate,
- 300 • host or service certificates,
- 301 • robot certificates.

302 RA Operators and CA Operators must both authenticate using valid
303 certificates to be able to access the RA Operator interface and CA Operator
304 interface, respectively.

305 **2.6.4 Repositories**

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

307 **2.7 Compliance Audit**

308 **2.7.1 Frequency of entity compliance audit**

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

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

314 **2.7.2 Identity/qualifications of auditor**

315 No stipulation.

316 **2.7.3 Auditor's relationship to audited party**

317 An external audit can be requested by any UK government department or
318 UK academic institution, or peer CA, or major relying Grid. The auditor
319 can be chosen by the requestor but the CA may require evidence of auditor's
320 qualifications. The CA reserves the right to impose confidentiality restric-
321 tions upon the auditor, for both security and DPA reasons.

322 **2.7.4 Topics covered by audit**

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

325 **2.7.5 Actions taken as a result of deficiency**

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

328 **2.7.6 Communication of results**

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

331 **2.8 Confidentiality**

332 The e-Science CA collects a Subscriber's name and e-mail address. The Sub-
333 scriber's name as defined in 3.1.2-3, and e-mail address are included in the
334 issued personal certificate (server certificates include email address). In ad-
335 dition, the RA keeps a copy of the photo id that was used by the Subscriber
336 to verify his/her identity. By making an application for a certificate a Sub-
337 scriber is deemed to have consented to their personal data being stored and
338 processed, subject to the Data Protection Act 1998 (see section B.1) and
339 Appendix B.1 of this document.

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

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

344 **2.8.1 Types of information to be kept confidential**

345 The information provided by the Subscriber to verify his/her identity will be
346 kept confidential.

347 **2.8.2 Types of information not considered confidential**

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

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

353 **2.8.3 Disclosure of certificate revocation/suspension in-** 354 **formation**

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

357 **2.8.4 Release to law enforcement officials**

358 The CA will not disclose confidential information to any third party unless
359 authorised to do so by the Subscriber or when required by law enforcement

360 officials who exhibit regular warrant.

361 **2.8.5 Release as part of civil discovery**

362 No stipulation.

363 **2.8.6 Disclosure upon owner's request**

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

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

373 **2.8.7 Other information release circumstances**

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

376 **2.9 Intellectual Property Rights**

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

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

381 Section 2.8 contains text derived from, or copied from, the UK Depart-
382 ment of Trade and Industry (DTI) supplementary example agreements from
383 the Lambert Working Group on Intellectual Property, and from the DTI
384 Office of Science and Technology LINK CBI/AURIL model collaboration
385 agreement.

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

389 This document typeset with L^AT_EX.

390 Chapter 3

391 IDENTIFICATION AND 392 AUTHENTICATION

393 3.1 Initial Registration

394 3.1.1 Types of names

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

398 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.

Robot	As person, except an additional CN is added to the name to indicate that the certificate is a robot certificate, and to indicate the type of robot.
-------	---

399

400 Common Names (CNs) must be encoded as `PrintableStrings` ([WCHK97],[HKYR95]).
 401 The maximal length of the CN is 64 characters for all types of certificates.
 402 The character set allowed for Common Names in personal certificates is

403 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

404 that is, Space (blank), decimal digits, lower and upper case US ASCII letters,
 405 left and right round brackets, and hyphen.

406 Robot certificate names satisfy the same constraints as personal certifi-
 407 cates except that the additional CN, identifying the certificate as a robot
 408 certificate and the type of the robot, begins with 'Robot:' (including the
 409 semicolon, which cannot occur in other types of certificates). This string is
 410 followed by the *type* of the robot, which is always a string consisting of letters.
 411 Additional text may be contained in the CN for disambiguation purposes, in
 412 which case a space separates the type from the disambiguation string.

413 For host and service certificates, the following characters are permitted:

414 '0' - '9', 'a' - 'z', 'A' - 'Z', '-', '.'

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

418 Email address in server and service certificates must be structured ac-
 419 cording to RFC822 and must be in the "addr-spec" format as defined in
 420 RFC822. The maximal length of an email address is 128 characters. Email
 421 addresses must be encoded as `IA5String` in the name but must not contain
 422 control characters or delete. For personal certificates, email addresses in sub-
 423 ject alternative name must be included as `rfc822Name` and satisfy the same
 424 constraints.

425 See also 7.1.4.

3.1.2 Need for names to be meaningful

Personal and Robot certificates

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

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

The CN of a personal certificate may contain additional text other than the Subscriber's authenticated name, in order to disambiguate between different users with the same name, or to allow the same user to have more than one certificate. The additional text must be formatted in such a way so as not to be confused with the Subscriber's name; it is recommended that it follows the Subscriber's name, with a space as separator, and enclosed in parentheses. The CA does not otherwise enforce or validate the content of this text, and RPs are explicitly forbidden to rely on the content of this additional text, or attribute any semantic value to it, for any authentication or authorisation purposes (see section 2.1.4).

The DN of any Robot certificate is that of the user who requested the certificate, with an additional CN identifying that the certificate identifies a robot, and the type of robot. A robot CN may also contain a disambiguating string for the case where a single person needs to have more than one robot certificate of the same type.

There is one exception to this rule, namely the certificate with the DN

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

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

Host and Service certificates

The CN in host and service certificates must be the Fully Qualified Domain Name (FQDN) of the host on which the credentials will be installed, formatted according to RFC1034 [Moc87].

459 **3.1.3 Rules for interpreting various name forms**

460 No stipulation.

461 **3.1.4 Uniqueness of names**

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

470 The e-Science CA will ensure that a DN is not reused. If a person re-
471 quests a certificate with the same DN as an existing certificate (regardless
472 of the status of this certificate) and the request is not a renewal or rekey,
473 the RA Operator will consult the original Personal Information to ensure
474 that the Subscriber is the same as the person who was identified in the orig-
475 inal certificate. If this identity cannot be established, the DN will never be
476 reused.

477 **3.1.5 Name claim dispute resolution procedure**

478 No stipulation.

479 **3.1.6 Recognition, authentication and role of trade-** 480 **marks**

481 No stipulation.

482 **3.1.7 Method to prove possession of private key**

483 Requests are submitted either as PKCS#10 or SPKAC. In either case, the
484 signature is verified by the CA.

485 3.1.8 Authentication of organisation identity

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

489 There is no verification of individuals' organisation identity.

490 3.1.9 Authentication of individual identity

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

493 In either case the Subscriber selects which RA is to carry out the identi-
 494 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).
Host	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).
Robot	The Subscriber must prove that the private key is adequately protected (section 2.1.3), and that the robot DN contains the Subscriber's personal DN (section 3.1.2).

495 When submitting a request to the CA, the Subscriber types a PIN – a

496 personal string known only to the Subscriber. When the Subscriber verifies
497 his or her identity to the RA Operator, the Operator can check the PIN to
498 ensure that the request he or she is about to approve was the one made by
499 the Subscriber. Only one-way hashes of the PINs are processed by the CA
500 and seen by the RA Operator (unless the Subscriber chooses to reveal it to
501 the RA Operator).

502 For certificates that contain an object signing extension, the CA does
503 not check, and makes no assertion, that the user is trustworthy as a software
504 developer or deployer. RPs must check the authenticated identity and decide
505 independently whether to run the signed software.

506 Certificate requests verified by the CA have `OU=Authority`, `L=CLRC` as
507 RA identifier.

508 **3.2 Routine Re-key**

509 Identity is proved using the existing credentials. Thus, the DN of the new
510 request must match the DN of the certificate used to submit the request.

511 **3.3 Re-key After Revocation**

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

514 **3.4 Revocation Request**

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

519 Authenticated certificate revocation requests may be made by

- 520 • The RA using:
 - 521 – Signed Email to the CA Manager;
 - 522 – Other secure method, as specified in the RA Operator's procedure.
- 523 • The Subscriber by:

- Mailing the CA manager directly by Signed Email.

525 Chapter 4

526 OPERATIONAL 527 REQUIREMENTS

528 4.1 Certificate Application

529 The Subscriber has to generate his/her own key pair. The minimum key
530 length is 1024 bits. Personal and robot certificates must not be shared; server
531 certificates must be linked to a single network entity. Maximal lifetime of a
532 certificate is 395 days. The default validity period is the maximum.

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

534 A valid personal certificate must be used (and in particular, the Sub-
535 scriber must prove possession of the corresponding private key) to submit a
536 request for the following types of certificates:

- 537 • a rekey of the same certificate,
- 538 • host or service certificates,
- 539 • robot certificates.

540 For robot certificate requests, the requestor must prove to the RA that a
541 secure key token is used to hold the private key.

542 The certificate used to request a rekey must have the same DN as that of
543 the request.

544 4.2 Certificate Issuance

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

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

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

554 Once a certificate request has been approved by the RA or the CA, the
555 certificate is normally issued by the CA within one working day.

556 If the authentication is unsuccessful, the certificate is not issued and an
557 e-mail with the reason is sent to the Subscriber or the Subscriber is otherwise
558 notified by CA or RA staff. In particular, the CA or RA may delete a request
559 if the Subscriber has made no attempt to authenticate him- or herself within
560 30 days of submitting the request.

561 All issued certificates are issued under the CP/CPS valid at the time of
562 issuance.

563 4.3 Certificate Acceptance

564 No stipulation.

565 4.4 Certificate Suspension and Revocation

566 4.4.1 Circumstances for revocation

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

- 570 1. The CA is informed that the Subscriber has ceased to be a member of
571 or associated with a UK e-Science program or activity;
- 572 2. the Subscriber's private key is lost or suspected to be compromised;

- 573 3. the information in the Subscriber’s certificate is wrong or inaccurate,
574 or suspected to be wrong or inaccurate;
- 575 4. the Subscriber violates his/her obligations.

576 It is worth noting that items 1 and 4 above may entail a revocation of *all*
577 the Subscriber’s certificates; in the case of item 4, depending on the nature
578 of the violation. The CA may provide facilities for the Subscriber to “hand
579 over” a host or service certificate to a successor, if the reason for revocation
580 is reason 1, provided this can be done without invalidating the information
581 in the certificate. In this case, the RA will verify that the successor is a
582 responsible administrator of the host or service in question. Robot certificates
583 tied to the Subscriber’s identity will always be revoked.

584 4.4.2 Who can request revocation

585 A certificate revocation can be requested by:

- 586 • The Registration Authority which authenticated the holder of the cer-
587 tificate;
- 588 • the holder of the certificate;
- 589 • any person presenting proof of knowledge that the Subscriber’s private
590 key has been compromised or that the Subscriber’s data have changed.

591 4.4.3 Procedure for revocation request

592 A revocation request is accepted if:

- 593 • The revocation request is signed with the key corresponding to certifi-
594 cate whose revocation is requested; or,
- 595 • The revocation request is signed by the RA who originally approved
596 the certificate request.

597 Any other revocation request is accepted only if the entity requesting the
598 revocation is properly authenticated.

599 **4.4.4 Revocation request grace period**

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

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

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

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

610 **4.4.5 Circumstances for suspension**

611 The CA does not offer suspension services.

612 **4.4.6 Who can request suspension**

613 No stipulation.

614 **4.4.7 Procedure for suspension request**

615 No stipulation.

616 **4.4.8 Limits on suspension period**

617 No stipulation.

618 **4.4.9 CRL issuance frequency**

619 CRLs are updated and re-issued within one hour after every approved cer-
620 tificate revocation, but at least once every week.

621 **4.4.10 CRL checking requirements**

622 No stipulation.

623 **4.4.11 On-line revocation/status checking availability**

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

625 **4.4.12 On-line revocation checking requirements**

626 No stipulation.

627 **4.4.13 Other forms of revocation advertisements avail-**
628 **able**

629 No stipulation.

630 **4.4.14 Checking requirements for other forms of revo-**
631 **cation advertisements**

632 No stipulation.

633 **4.4.15 Special requirements re key compromise**

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

638 **4.5 Security Audit Procedures**

639 **4.5.1 Types of event recorded**

640 The following events are recorded:

- 641 ● certification requests;
- 642 ● issued certificates;
- 643 ● requests for revocation;
- 644 ● issued CRLs;
- 645 ● login/logout/reboot of the signing machine.

646 **4.5.2 Frequency of processing log**

647 No stipulation.

648 **4.5.3 Retention period for audit log**

649 The minimum retention period is 3 years.

650 **4.5.4 Protection of audit log**

651 No stipulation.

652 **4.5.5 Audit log backup procedures**

653 No stipulation.

654 **4.5.6 Audit collection system (internal vs external)**

655 No stipulation.

656 **4.5.7 Notification to event-causing subject**

657 No stipulation.

658 **4.5.8 Vulnerability assessments**

659 No stipulation.

660 **4.6 Records Archival**

661 **4.6.1 Types of event recorded**

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

- 663 • certification requests;
- 664 • issued certificates;

- 665 • requests for revocation;
- 666 • issued CRLs;
- 667 • all e-mail messages received by the CA (not the confirmation messages
668 sent to the Subscribers);
- 669 • all e-mail messages sent by the CA;
- 670 • all documents appointing CA and RA Staff.

671 Each RA must log the following:

- 672 • for each approved request, how it was approved;
- 673 • for each rejected request, why it was rejected;
- 674 • for each approved revocation request, the reason for revocation;
- 675 • for each rejected revocation request, the reason for revocation and the
676 reason the request was rejected.

677 **4.6.2 Retention period for archive**

678 The minimum retention period is 3 years.

679 **4.6.3 Protection of archive**

680 No stipulation.

681 **4.6.4 Archive backup procedures**

682 No stipulation.

683 **4.6.5 Requirements for time-stamping of records**

684 No stipulation.

685 **4.6.6 Archive collection system (internal or external)**

686 No stipulation.

687 **4.6.7 Procedures to obtain and verify archive informa-**
688 **tion**

689 No stipulation.

690 **4.7 Key Changeover**

691 The CA will generate a new key pair and obtain a new CA certificate from
692 the Root one year and 30 days (the maximal lifetime of a Subscriber's cer-
693 tificate) before the expiry of the CA certificate. In the final year the CA's
694 old certificate will be available for validation purposes only, whereas new
695 certificates and CRLs will be signed with the new CA key.

696 **4.8 Compromise and Disaster Recovery**

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

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

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

705 **4.8.1 Computing resources, software, and/or data are**
706 **corrupted**

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

708 **4.8.2 Entity public key is revoked**

709 No stipulation.

710 **4.8.3 Entity key is compromised**

711 No stipulation.

712 **4.8.4 Secure facility after a natural or other type of**
713 **disaster**

714 No stipulation.

715 **4.9 CA Termination**

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

- 717 • inform the Registration Authorities, Subscribers, Relying Parties, and
718 cross-certifying CAs of which the CA is aware;
- 719 • make information of its termination widely available;
- 720 • stop issuing certificates.

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

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

731 Chapter 5

732 PHYSICAL, PROCEDURAL, 733 AND PERSONNEL 734 SECURITY CONTROLS

735 5.1 Physical Controls

736 5.1.1 Site location and construction

737 No stipulation.

738 5.1.2 Physical access

739 The CA operates in a controlled environment, where access is restricted to
740 authorised people and logged. The signing machine is connected to the online
741 machine via a private and monitored network. The signing machine has a
742 the private key stored in an HSM with certification to FIPS-140-2 Level 3.

743 5.1.3 Power and air conditioning

744 The online machine and all other machines on the CA's private network
745 including the signing machine operates in an air conditioned environment
746 and are not rebooted or power-cycled except for essential maintenance.

747 **5.1.4 Water exposures**

748 No stipulation.

749 **5.1.5 Fire prevention and protection**

750 No stipulation.

751 **5.1.6 Media storage**

752 No stipulation.

753 **5.1.7 Waste disposal**

754 No stipulation.

755 **5.1.8 Off-site backup**

756 No stipulation.

757 **5.2 Procedural Controls**

758 **5.2.1 Trusted roles**

759 No stipulation.

760 **5.2.2 Number of persons required per task**

761 No stipulation.

762 **5.2.3 Identification and authentication for each role**

763 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. Normally, the L field identifies the Department where the Manager is appointed, but the L can also be used further to subdivide the RA in the case of very large or physically distributed RAs managed by a single manager. 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.

796 **5.3.3 Training requirements**

797 No stipulation.

798 **5.3.4 Retraining frequency and requirements**

799 No stipulation.

800 **5.3.5 Job rotation frequency and sequence**

801 No stipulation.

802 **5.3.6 Sanctions for unauthorized actions**

803 In the event of unauthorised actions, abuse of authority or unauthorised use
804 of entity systems by the CA or RA Operators, the CA manager may revoke
805 the privileges concerned.

806 **5.3.7 Contracting personnel requirements**

807 No stipulation.

808 **5.3.8 Documentation supplied to personnel**

- 809 • It is the responsibility of the CA Manager to provide the CA Operators
810 with a copy of the “e-Science CA Operator’s Procedure”.
- 811 • It is the responsibility of the CA Manager to provide the RA Manager
812 with a copy of the “e-Science RA Manager’s Procedure”.
- 813 • It is the responsibility of the RA Manager to provide the RA Operator
814 with a copy of the “e-Science RA Operator’s Procedure”.

815 Chapter 6

816 TECHNICAL SECURITY 817 CONTROLS

818 6.1 Key Pair Generation and Installation

819 6.1.1 Key pair generation

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

822 6.1.2 Private key delivery to entity

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

825 6.1.3 Public key delivery to certificate issuer

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

828 6.1.4 CA public key delivery to subscribers

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

831 **6.1.5 Key sizes**

832 Keys of length less than 1024 bits are not accepted. The CA key is of length
833 2048 bits.

834 **6.1.6 Public key parameters generation**

835 No stipulation.

836 **6.1.7 Parameter quality checking**

837 No stipulation.

838 **6.1.8 Hardware/software key generation**

839 If the private key is protected by a hardware token, it must be generated on
840 that token.

841 **6.1.9 Key usage purposes (as per X.509 v3 key usage 842 field)**

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

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

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

848 **6.2 Private Key Protection**

849 The following table summarises how Subscribers' private keys must be pro-
850 tected, depending on the type and use of the corresponding certificate. Other
851 protection methods are permissible if they are equivalent or stronger.

Type	Personal	Host	Service	Robot
file system, user only			■	
file system, root only		■	■	
file system, encrypted, Subscriber only	■	■	■	
key token	■	■	■	■

852

853

The protections above are to be interpreted as follows:

854

- **File system, user only:**

855

- The private key is protected by file system access control, in such a way that only its primary user can access it.

856

857

- The primary user need not be the same as the Subscriber (who is responsible for the certificate), but must have been granted access by the Subscriber.

858

859

860

- The Subscriber must be responsible for the host in which the credentials are installed, and must be responsible for granting and revoking privileged access (who can potentially bypass file protection) to the filesystem to others.

861

862

863

864

- **File system, root only:**

865

- The private key is protected by file system access control, in such a way that only privileged users can access it.

866

867

- The key may be stored in a system-user account, provided no non-privileged users can read the key from that account.

868

869

- The Subscriber must be responsible for the host in which the credentials are installed, and must be responsible for granting and revoking privileged access (who can potentially bypass file protection) to the filesystem to other users.

870

871

872

873

- **File system, encrypted, Subscriber only:**

874

- Only encrypted versions of the private key may be stored on permanent media, and they must be protected by file system access controls.

875

876

- 877 – The symmetric encryption key should be generated from a Strong
878 passphrase, using PKCS#5 version 2.0 or later; if another en-
879 ryption method is used, the other method must be equivalent or
880 stronger.
- 881 – Users should make best endeavours that the encrypted key is not
882 copied around or stored on shared filesystems.

- 883 • **Key token:**

- 884 – The key token protecting the private key must satisfy the con-
885 straints of section 6.2.1.

886 **6.2.1 Standards for cryptographic module**

887 The CA's private key is protected by an HSM certified to FIPS 140-2 Level
888 3.

889 A key token, when used to protect Subscribers' private keys (section 6.2),
890 must be certified to FIPS 140-1 Level 2 or higher, or FIPS 140-2 Level 2 or
891 higher.

892 **6.2.2 Private key (n out of m) multi-person control**

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

895 Backup copies of the CA's private key is under (3 out of 5) multi-person
896 control (as well as locked in a safe as described in 6.2.4).

897 **6.2.3 Private key escrow**

898 Private keys must not be escrowed.

899 **6.2.4 Private key backup**

900 The private key of the CA is encrypted within the HSM using keys held
901 on secure key tokens (see also section 6.2.2). The backup copy can thus be
902 backed up normally with the rest of the filesystem and databases (but of
903 course with access controls on the backups).

904 **6.2.5 Private key archival**

905 No stipulation.

906 **6.2.6 Private key entry into cryptographic module**

907 The CA's private key is generated inside the HSM and never leaves it in
908 unencrypted form.

909 A Subscriber's private key, when protected by a key token, must be gen-
910 erated in that token.

911 **6.2.7 Method of activating private key**

912 Each CA Operator has a key token which activates the private key for signing.
913 The Operator inserts the token when he or she will be signing, and types a
914 PIN to activate the key token.

915 **6.2.8 Method of deactivating private key**

916 The key token (see section 6.2.7) is removed from the interface when the CA
917 Operator has finished signing certificates and CRLs, thus deactivating the
918 private key.

919 **6.2.9 Method of destroying private key**

920 No stipulation.

921 **6.3 Other Aspects of Key Pair Management**

922 **6.3.1 Public key archival**

923 The CA archives all issued certificates and all its own public and private keys
924 since 5 Aug 2002 (date of going to production).

925 **6.3.2 Usage periods for the public and private keys**

926 Subscribers' certificates have a validity period of one year plus 30 days. The
927 CA certificate has a validity period of five years.

928 **6.4 Activation Data**

929 The CA's private key is protected as described in the previous sections. If
930 Subscriber's private key is protected by a passphrase, it must be a Strong
931 passphrase; if protected by a key token, it must have a PIN known only to
932 the Subscriber to activate it.

933 **6.4.1 Activation data generation and installation**

934 No stipulation.

935 **6.4.2 Activation data protection**

936 See section 6.4.

937 **6.4.3 Other aspects of activation data**

938 No stipulation.

939 **6.5 Computer Security Controls**

940 **6.5.1 Specific computer security technical requirements**

941 The CA server and all other machines on the CA's private subnet, including
942 the signing machine, are secured as follows:

- 943 • operating systems are maintained at a high level of security by applying
944 in a timely manner all recommended and applicable security patches;
- 945 • monitoring is done to detect unauthorised software changes;
- 946 • the private network is monitored to detect unauthorised activity;
- 947 • services are reduced to the bare minimum.

948 The CA has a security document describing in detail the security infrastruc-
949 ture and logging. For security reasons, this document is available only to CA
950 staff, relevant site operational security staff, and auditors.

951 **6.5.2 Computer security rating**

952 No stipulation.

953 **6.6 Life-Cycle Technical Controls**

954 **6.6.1 System development controls**

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

957 **6.6.2 Security management controls**

958 No stipulation.

959 **6.6.3 Life cycle security ratings**

960 No stipulation.

961 **6.7 Network Security Controls**

962 Certificates are generated on a machine connected to a private, dedicated,
963 network, located in a secure environment and managed by a suitably trained
964 person. All machines are protected by suitably configured firewalls.

965 **6.8 Cryptographic Module Engineering Con-**
966 **trols**

967 No stipulation.

968 Chapter 7

969 CERTIFICATE AND CRL 970 PROFILES

971 7.1 Certificate Profile

972 7.1.1 Version number

973 X.509.v3

974 7.1.2 Certificate extensions

975 Host and service certificates have the same extensions.

976 Robot certificates can have different extensions, depending on the type
977 and use of the robot. Each type of robot and its certificate profile is docu-
978 mented in detail in a separate document available from the CA's web site.

979 In any case, the extensions accorded to robot certificates is a (not neces-
980 sarily proper) subset of those accorded to Personal certificates, *except* that:

- 981 • robot certificates may have extended key usage set;
- 982 • robot certificates have a *second* OID in their PolicyInformation, namely,
983 that of the robot 1SCP under which they are issued (that of the CP/CPS
984 under which they are issued is the first).

985 **End Entity certificate profile:**

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
Subject Alternative Name (personal/robot)	Subject's personal email address
Subject Alternative Name (server/service)	Server's Fully Qualified Domain Name
Issuer Alternative Name	CA email
CRL Distribution Points	HTTP URL of CRL
Netscape Cert Type	Personal, Robot: SSL Client, S/MIME Personal: (optionally) object signing Server, service: SSL Client, SSL Server
Netscape Comment	"UK e-Science XXX Certificate" where "XXX" is "User", "Host", "Service", or "Robot".
Netscape CA Revocation URL	HTTP URL of CRL
Netscape Revocation URL	HTTP URL of CRL

Signature Algorithm	sha1WithRSAEncryption
---------------------	-----------------------

986 The CA operator certificate (see section 3.1.2) has the same extensions as a
 987 user certificate. It always has the Netscape Object Signing extension set.

988 **CA certificate profile:**

Basic Constraints	<i>critical</i> CA:TRUE
Key Usage	<i>critical</i> keyCertSign, cRLSign
Subject Key Identifier	hash
Authority Key Identifier	keyid
Signature Algorithm	sha1WithRSAEncryption

989 **7.1.3 Algorithm object identifiers**

990 No stipulation.

991 **7.1.4 Name forms**

992 **CA certificate**

993 Issuer:

994 /C=UK/O=eScienceRoot/OU=Authority/CN=UK e-Science Root

995 Subject:

996 /C=UK/O=eScienceCA/OU=Authority/CN=UK e-Science CA

997 Note that the subject has /C=UK/O=eScienceCA/* to avoid having the
 998 root sign in the same namespace as the CA described in this CP/CPS.

999 **End Entity Certificate**

1000 Issuer: is the CA's subject DN.

1001 Subject: The subject field contains the Distinguished Name of the entity
1002 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	Personal and robot: Name and surname of Subscriber; Host: FQDN of host; Service: FQDN of host prefixed by the service name (see 7.1.5) and a '/' (e.g. CN=ldap/ldap.rl.ac.uk).
CommonName	Robots have an additional CN of the form Robot : <i>type</i> .
SubjectAltName	FQDN of server

1003 Important notes:

- 1004 • The DN of EEs is preserved across the CA certificate rollover.
- 1005 • The CN in a personal certificate may contain additional text string,
1006 as described in section 3.1.2. Likewise, the additional robot CN may
1007 contain an additional text string, as described in the same section.

1008 The name of the special CA operator (see section 3.1.2) certificate is

1009 /C=UK/O=eScience/OU=Authority/L=CLRC/CN=ca-operator

1010 The email address in host and service certificates must be that of one
1011 or more people responsible for the server in question, and need not be a
1012 personal address. Host certificates should not have “host” as a service, i.e.
1013 they should have `CN=host.univ.ac.uk` and not `CN=host/host.univ.ac.uk`
1014 if they are used with non-Globus servers.

1015 The CA will issue certificates for a given service if and only if:

- 1016 • the service has been defined by IANA [IAN]; or
- 1017 • The CA Manager has approved the service.

1018 It is the responsibility of the CA Manager to define the non-IANA services
1019 allowed by the CA. For each service, the CA Manager must provide

- 1020 • the name of the service,
- 1021 • the default port number,
- 1022 • a short description of the service,
- 1023 • a reference URI.

1024 The CA Manager must ensure that services are unique in name.

1025 It is the responsibility of the CA Manager to define the robot types sup-
1026 ported by the CA. For each robot type, the CA Manager must provide

- 1027 • the name of the robot type (as in `CN=Robot: type`);
- 1028 • The exact profile of the robot (extensions);
- 1029 • Purposes for which the robot certificate is to be used;
- 1030 • Purposes for which using the robot certificate is explicitly forbidden, if
1031 any;
- 1032 • Additional qualifications a requestor must have and prove to an RA in
1033 order to successfully obtain a robot certificate, if any.

1034 7.1.5 Name constraints

1035 No stipulation¹.

¹Note: The text that used to be in this section has been moved to the more appropriate previous sections (Name Forms, above)

1036 **7.1.6 Certificate policy Object Identifier**

1037 Certificates contain in the PolicyInformation extension the policyIdentifier
1038 containing the OID of the CP/CPS under which they were issued. Addition-
1039 ally, robot certificates contain an 1SCP robot OID.

1040 **7.1.7 Usage of Policy Constraints extensions**

1041 No stipulation.

1042 **7.1.8 Policy qualifier syntax and semantics**

1043 No stipulation.

1044 **7.1.9 Processing semantics for the critical certificate** 1045 **policy**

1046 No stipulation.

1047 **7.2 CRL Profile**

1048 **7.2.1 Version number**

1049 X.509.v1: Version 1 is required for compatibility with Netscape Communi-
1050 cator.

1051 **7.2.2 CRL and CRL Entry Extensions**

1052 No stipulation.

1053 Chapter 8

1054 SPECIFICATION 1055 ADMINISTRATION

1056 8.1 Specification Change Procedures

1057 We distinguish between different types of modifications to the CP/CPS:

1058 *Editorial updates:* editorial changes to the CPS, including replacing fields
1059 with “No stipulation”, as long as they do not affect procedure or compromise
1060 security. These changes are announced on the CA web site but no advance
1061 warning will be given.

1062 *Procedure updates:* minor changes to the CPS that do not compromise secu-
1063 rity in any way. E.g. changes to the verification or issuing procedure that
1064 do not affect security. Subscribers and relying parties will not be warned of
1065 such changes in advance but RAs will be given at least one week’s notice of
1066 changes that affect their procedures.

1067 *Technical updates:* e.g. changes to the extensions in the issued certificates.
1068 Such changes will be announced on the CA web site and on appropriate
1069 mailing lists at least 14 days in advance.

1070 *Security updates:* changes that affect the security, e.g. changes to the minimal
1071 requirements for verifying requests, or changing the key sizes. These changes
1072 will be announced at least 30 days in advance on the CA web site, and to
1073 appropriate mailing lists, including the EU Grid PMA mailing list. However,
1074 urgent security fixes may be carried out without advance warning and then
1075 documented in the CPS. These will be announced in the same manner.

1076 *Policy updates:* e.g. changes to the namespace, or introducing subordinate
1077 CAs. A proposal will be announced at least 30 days in advance on the CA

1078 web site and appropriate mailing lists.

1079 *Termination:* A scheduled termination of the CA is announced on the CA
1080 web site and appropriate mailing lists at least 60 days in advance.

1081 **8.2 Publication and Notification Policies**

1082 This CP/CPS is available at [CAW]. All changes are announced on the CA
1083 web site and a changelog is available. In addition, changes are announced to
1084 appropriate mailing lists, depending on the type of change, as described in
1085 section 8.1.

1086 There is a mailing list for RA Managers and Operators. Only subscribers
1087 can post to the mailing list. Only subscribers can read the archives.

1088 **8.3 CPS Approval Procedures**

1089 No stipulation.

1090 Appendix A

1091 Revision History

1092

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.
1.3	1.7	4 August 2006	CA rollover, signing key online, robots.
1.4	1.8	26 Nov 2007	Security rollover, plus minor security-related updates (only). 2nd update fixed year.

1093

1094 The OID in the table is the final two digits of the actual OID, as defined in
1095 section 1.2.

1096 Appendix B

1097 Compliance with Laws and 1098 Regulations

1099 The UK e-Science CA operates under English Law. See section 2.4.1.

1100 In the case an RA Operator or CA Operator cannot complete his or her
1101 operations without violating rules set forth in this Appendix, the Operator
1102 must not complete the operation and must notify the CA Manager, and, if
1103 applicable, his or her RA Manager.

1104 B.1 The Data Protection Act

1105 The Data Protection Act 1998 (DPA) [DPA00].

1106 B.1.1 Definitions

- 1107 • The *data controller* is the CA Manager, the person mentioned in 1.4.2.
- 1108 • The *data processor* is any RA Manager or Operator.
- 1109 • The *data subject* is a Subscriber requesting a certificate, or an RA
1110 Operator or a CA Operator being appointed as such by the CA.
- 1111 • *Data* is to be understood as defined in DPA section I.1.
- 1112 • *Processing Data* is to be understood as defined in DPA section I.1.
- 1113 • Throughout this Appendix, *Personal Data* means Data which is Per-
1114 sonal Data as defined in DPA section I.1 but which is not *Sensitive*
1115 *Personal Data* as defined in DPA section I.2.

- 1116 • *Personal Information* is defined in section 1.1.1 of this document. For
1117 the purposes of the DPA,
- 1118 – the photo id is considered Sensitive Personal Data;
- 1119 – all other parts of Personal Information are considered Personal
1120 Data.

1121 B.1.2 Preliminaries

1122 The *intent* of Processing Data by the UK e-Science CA is that minimal and
1123 adequate Personal Information is stored and Processed in order that the UK
1124 e-Science CA may operate according to the policy and practices described
1125 in this CP/CPS, including being an internationally approved medium level
1126 CA.

1127 B.1.3 Data

1128 The UK e-Science CA stores the following Data:

- 1129 1. The CA publishes on its web page, and may publish by other methods,
1130 the Subscriber's *certificate* and thus all information contained therein,
1131 including the Subscriber's name;
- 1132 2. The CA logs and stores all Subscriber and RA interactions with the
1133 CA's online service, in order to satisfy the requirements of sections 4.5
1134 and 4.6 of this CP/CPS;
- 1135 3. The RA Operator Processes Personal Information, and possibly other
1136 Data, as described in section B.1.5;
- 1137 4. The CA stores authorisation information about the RA Manager and
1138 Operators sufficient to convince the CA that the RA Manager and
1139 Operators satisfy the conditions of section 5.3.1 and that the CA has the
1140 RA Manager's assurance that the RA Operator will operate according
1141 to this CP/CPS;
- 1142 5. For host and service certificates, it may be necessary to obtain and store
1143 Personal Data that proves to the RA Operator's satisfaction that Sub-
1144 scriptioner is responsible system administrator for the resource for which
1145 the Subscriber requests a certificate, in accordance with sections 2.1.2,
1146 2.1.3, and 3.1.9;

1147 6. It may be necessary to obtain and store Personal Data to prove to the
1148 RA Operator's satisfaction that the Subscriber is entitled to a certifi-
1149 cate from the UK e-Science CA, cf. section 1.3.3.

1150 Notwithstanding the above, the Data Processed by the UK e-Science CA is
1151 subject to the following restrictions:

- 1152 • The UK e-Science CA must not Process or attempt to Process any
1153 Sensitive Personal Data *except* the photo id.
- 1154 • Personal Data and Sensitive Personal Data must be relevant and ade-
1155 quate for the purpose for which it is Processed.
- 1156 • The UK e-Science CA must Process Personal Information only as de-
1157 fined in this Appendix, and in accordance with the DPA.

1158 **B.1.4 Consent**

1159 By submitting Data to the online CA ([CAW]), the Subscriber is considered
1160 to have given consent that the submitted Data may be Processed by the
1161 e-Science CA (there is a notice to this effect on the web page). By present-
1162 ing Personal Information to the RA Operator, the Subscriber is deemed to
1163 have given consent that this information may be Processed according to the
1164 purposes described in this document, and stored according to the procedures
1165 described in this document (there is a notice to this effect on the web page).
1166 By applying for RA Operator or CA Operator status, the RA Operator or CA
1167 Operator is deemed to have consented that the CA can Process the Data as
1168 described below (there is a notice to this effect in the template appointment
1169 letters provided by the CA).

1170 **B.1.5 Processing**

1171 The CA permits that Personal Information is Processed as follows:

- 1172 1. The CA Operator or RA Operator obtains Personal Information or
1173 other Data from the Subscriber or from another Operator relevant and
1174 adequate for the purposes described below;
- 1175 2. A photocopy of the Personal Information is made for the purposes
1176 described below;

- 1177 3. The photocopy of Personal Information is subsequently accessed only
1178 for the purposes described below;
- 1179 4. Subscriber's email address is obtained and used only for the purposes
1180 described below;
- 1181 5. Relevant and adequate information is Processed to satisfy section 4.5
1182 of this CP/CPS in accordance with sections 4.5 and 4.6.

1183 **B.1.6 Purpose**

1184 The UK e-Science CA Processes Personal Information for the following pur-
1185 poses:

- 1186 1. Identification of a Subscriber;
- 1187 2. Subsequent auditing of the Identification process, for the case where the
1188 UK e-Science CA must prove the link from the DN to the Subscriber's
1189 real identity;
- 1190 3. Release of Personal Information under the circumstances described in
1191 section 2.8 and according to the procedures described in the same sec-
1192 tion;
- 1193 4. To maintain the uniqueness of the DN to the extent described in sec-
1194 tion 3.1.4;
- 1195 5. For RA and CA Operators, to check to the CA Manager's satisfaction
1196 that the RA or CA Operator is duly authorised by appointment letter
1197 to operate according to this CP/CPS and that the RA Manager and
1198 Operator satisfy the conditions described in section 5.3.1;
- 1199 6. Adequate Personal Information is Processed to satisfy the auditing re-
1200 quirements set forth in sections 2.7, 4.5 and 4.6 of this CP/CPS;
- 1201 7. Email address is used only to notify the Subscriber that:
- 1202 • A new certificate has been issued to the Subscriber;
 - 1203 • A certificate held by the Subscriber is about to expire.

1204 Data may be used for statistical purposes

- 1205 • only with the Data Controller's permission; and

- 1206 • if there is reasonable cause; and
- 1207 • if the published information contain neither Personal Data nor Sensitive
1208 Personal Data, and no Personal Data or Sensitive Personal Data can
1209 be derived from it; and
- 1210 • the Processing associated with and required for statistical purposes are
1211 done in accordance with the DPA section 33.

1212 Any other use of Personal Information is explicitly forbidden.

1213 **B.1.7 Data Release**

1214 Circumstances requiring Processing of Personal Information include, but are
1215 not necessarily limited to, the following cases:

- 1216 1. A CA Manager or Operator is considered to have breached CA Obli-
1217 gations (section 2.1.1);
- 1218 2. An RA Manager or Operator is considered to have breached RA Obli-
1219 gations (section 2.1.2);
- 1220 3. A Subscriber is considered to have breached Subscriber's Obligations
1221 (section 2.1.3);
- 1222 4. Release of information as described in section 2.8, including any release
1223 required by UK law;
- 1224 5. Release of information as required for auditing purposes, including com-
1225 pliance audit as described in section 2.7.

1226 In each case, the UK e-Science CA shall ensure that only the adequate and
1227 relevant information is released and that the information is Processed law-
1228 fully and in accordance with the rules of sections B.1.5 and B.1.6, and in
1229 accordance with the DPA.

1230 **B.1.8 Data Maintenance**

1231 There is no requirement for keeping Personal Information Processed by the
1232 RA up to date, except to the extent required to satisfy the RA Operator
1233 that the information mentioned in 5 and 6 in section B.1.3 is still valid if and
1234 when certificates that required this information prior to their approval are
1235 being renewed.

1236 It is the RA Manager's responsibility to ensure that the Data Processed
1237 by the CA concerning his or her RA or any Manager or Operator associated
1238 with that RA is kept up to date, and inform the CA of any update.

1239 **B.1.9 Data Retention**

1240 Personal Information shall be kept by the UK e-Science CA for as long as is
1241 necessary:

- 1242 1. Personal Information used to obtain a personal certificate with a certain
1243 DN shall be kept for as long as the Subscriber has a valid certificate
1244 with this DN, including renewals of the certificate, and for a period
1245 beyond the expiry or revocation of the latest certificate held by the
1246 Subscriber necessary to satisfy the retention requirements described in
1247 section 4.6;
- 1248 2. Data used to obtain a host or service certificate shall be kept for as
1249 long as the Subscriber is responsible administrator for the resource for
1250 which the certificate was obtained, and for a period beyond the expiry
1251 or revocation of the latest certificate held by the Subscriber, or beyond
1252 the administrator rights being passed on to someone else, necessary to
1253 satisfy the retention requirements described in section 4.6.
- 1254 3. Data used by the CA Manager to authorise RA Managers and Op-
1255 erators must be kept for a period beyond the termination of the RA
1256 necessary to satisfy the requirements described in section 4.6. For the
1257 termination of the CA, the conditions in sections 4.6.2 and 4.9 apply.

1258 It is the responsibility of the RA Manager to ensure that appropriate techni-
1259 cal and organisational measures are taken against unlawful or unauthorised
1260 Processing of Data held by the RA. It is the responsibility of the CA Manager
1261 to ensure that appropriate technical and organisational measures are taken
1262 against unlawful or unauthorised Processing of Data held by the CA.

1263 **B.1.10 Data Termination**

1264 It is the responsibility of the RA Manager to ensure that Personal Information
1265 held and Processed by the RA is adequately destroyed by the end of the
1266 retention period. It is the responsibility of the CA Manager to ensure that
1267 Personal Information held and Processed by the CA is adequately destroyed
1268 by the end of the retention period.

Bibliography

- 1270 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate
1271 policy model. [http://www.gridforum.org/2_SEC/pdf/Draft-](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf)
1272 [GGF-CP-06.pdf](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf), September 2001.
- 1273 [BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform resource
1274 locators. <http://www.rfc-editor.org/rfc/rfc1738.txt>, December
1275 1994.
- 1276 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 1277 [Cec01] R. Cecchini. INFN CA CP/CPS. [http://security.fi.infn.it/CA/-](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf)
1278 [CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 1279 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-
1280 ture Certificate Policy and Certification Practices Framework.
1281 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 1282 [CFS⁺03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet
1283 x.509 public key infrastructure certificate policy and certification
1284 practices framework. [http://www.ietf.org/internet-drafts/draft-](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt)
1285 [ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 1286 [DPA00] Data protection act 1998. [http://www.legislation.hmso.gov.uk/-](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm)
1287 [acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm), March 2000.
- 1288 [Eur00] EuroPKI Certificate Policy. [http://www.europki.org/ca/root/-](http://www.europki.org/ca/root/cps/en_cp.pdf)
1289 [cps/en_cp.pdf](http://www.europki.org/ca/root/cps/en_cp.pdf), October 2000. Version 1.1.
- 1290 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-
1291 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,
1292 December 1999. Version 1.0.
- 1293 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.
1294 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.
1295 Version 1.1.

- 1296 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.
1297 <http://www.globus.org/security/v2.0/index.html>.
- 1298 [Glob] Globus. Grid security infrastructure for globus toolkit 3.
1299 <http://www.globus.org/security/GSI3/index.html>.
- 1300 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 1301 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String
1302 Representation of Standard Attribute Syntaxes. <http://www.rfc-editor.org/rfc/rfc1778.txt>, March 1995.
1303
- 1304 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public
1305 key infrastructure certificate and certificate revocation list (crl)
1306 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 1307 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 1308 [Moc87] P. Mockapetris. Domain names - concepts and facilities.
1309 <http://www.rfc-editor.org/rfc/rfc1034.txt>, November 1987.
- 1310 [NCS99] National Computational Science Alliance Certificate Pol-
1311 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html)
1312 [Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html), June 1999.
- 1313 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-](http://www.digsigtrust.com/-certificates/policy/tsindex.html)
1314 [certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 1315 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight
1316 Directory Access Protocol (v3): Attribute Syntax Definitions.
1317 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.