

UK e-Science Certification Authority
Certificate Policy and Certification Practices
Statement
ChangeLog Version 1.2-1.3-3

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

3 July 2006

Contents

1	INTRODUCTION	11
1.1	Overview	11
1.1.1	General definitions	11
1.2	Identification	16
1.3	Community and Applicability	17
1.3.1	Certification authorities	17
1.3.2	Registration authorities	17
1.3.3	End entities (Subscribers)	18
1.3.4	Applicability	18
1.4	Contact Details	18
1.4.1	Specification administration organisation	18
1.4.2	Contact person	18
1.4.3	Person determining CPS suitability for the policy	19
2	GENERAL PROVISIONS	21
2.1	Obligations	21
2.1.1	CA obligations	21
2.1.2	RA obligations	22
2.1.3	Subscriber obligations	23
2.1.4	Relying party obligations	25
2.1.5	Repository obligations	25
2.2	Liability	26
2.2.1	CA liability	26
2.2.2	RA liability	26
2.3	Financial Responsibility	26

2.3.1	Indemnification by relying parties	26
2.3.2	Fiduciary relationships	26
2.3.3	Administrative processes	27
2.4	Interpretation and Enforcement	27
2.4.1	Governing law	27
2.4.2	Severability, survival, merger, notice	27
2.4.3	Dispute resolution procedures	27
2.5	Fees	28
2.5.1	Certificate issuance or renewal fees	28
2.5.2	Certificate access fees	28
2.5.3	Revocation or status information access fees	28
2.5.4	Fees for other services such as policy information	28
2.5.5	Refund policy	28
2.6	Publication and Repositories	28
2.6.1	Publication of CA information	28
2.6.2	Frequency of publication	29
2.6.3	Access controls	29
2.6.4	Repositories	30
2.7	Compliance Audit	30
2.7.1	Frequency of entity compliance audit	30
2.7.2	Identity/qualifications of auditor	30
2.7.3	Auditor's relationship to audited party	30
2.7.4	Topics covered by audit	30
2.7.5	Actions taken as a result of deficiency	31
2.7.6	Communication of results	31
2.8	Confidentiality	31
2.8.1	Types of information to be kept confidential	31
2.8.2	Types of information not considered confidential	31
2.8.3	Disclosure of certificate revocation/suspension information	32
2.8.4	Release to law enforcement officials	32
2.8.5	Release as part of civil discovery	32
2.8.6	Disclosure upon owner's request	32

2.8.7 Other information release circumstances 32
2.9 Intellectual Property Rights 33

3 IDENTIFICATION AND AUTHENTICATION 35

3.1 Initial Registration 35
3.1.1 Types of names 35
3.1.2 Need for names to be meaningful 37
3.1.3 Rules for interpreting various name forms 38
3.1.4 Uniqueness of names 38
3.1.5 Name claim dispute resolution procedure 38
3.1.6 Recognition, authentication and role of trademarks . . 38
3.1.7 Method to prove possession of private key 38
3.1.8 Authentication of organisation identity 39
3.1.9 Authentication of individual identity 39
3.2 Routine Re-key 40
3.3 Re-key After Revocation 40
3.4 Revocation Request 40

4 OPERATIONAL REQUIREMENTS 43

4.1 Certificate Application 43
4.2 Certificate Issuance 44
4.3 Certificate Acceptance 44
4.4 Certificate Suspension and Revocation 44
4.4.1 Circumstances for revocation 44
4.4.2 Who can request revocation 45
4.4.3 Procedure for revocation request 45
4.4.4 Revocation request grace period 46
4.4.5 Circumstances for suspension 46
4.4.6 Who can request suspension 46
4.4.7 Procedure for suspension request 46
4.4.8 Limits on suspension period 46
4.4.9 CRL issuance frequency 46
4.4.10 CRL checking requirements 46
4.4.11 On-line revocation/status checking availability 47

4.4.12	On-line revocation checking requirements	47
4.4.13	Other forms of revocation advertisements available . . .	47
4.4.14	Checking requirements for other forms of revocation advertisements	47
4.4.15	Special requirements re key compromise	47
4.5	Security Audit Procedures	47
4.5.1	Types of event recorded	47
4.5.2	Frequency of processing log	48
4.5.3	Retention period for audit log	48
4.5.4	Protection of audit log	48
4.5.5	Audit log backup procedures	48
4.5.6	Audit collection system (internal vs external)	48
4.5.7	Notification to event-causing subject	48
4.5.8	Vulnerability assessments	48
4.6	Records Archival	48
4.6.1	Types of event recorded	48
4.6.2	Retention period for archive	49
4.6.3	Protection of archive	49
4.6.4	Archive backup procedures	49
4.6.5	Requirements for time-stamping of records	49
4.6.6	Archive collection system (internal or external)	49
4.6.7	Procedures to obtain and verify archive information . . .	50
4.7	Key Changeover	50
4.8	Compromise and Disaster Recovery	50
4.8.1	Computing resources, software, and/or data are cor- rupted	50
4.8.2	Entity public key is revoked	50
4.8.3	Entity key is compromised	50
4.8.4	Secure facility after a natural or other type of disaster .	51
4.9	CA Termination	51
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECUR- RITY CONTROLS	53
5.1	Physical Controls	53

5.1.1	Site location and construction	53
5.1.2	Physical access	53
5.1.3	Power and air conditioning	53
5.1.4	Water exposures	54
5.1.5	Fire prevention and protection	54
5.1.6	Media storage	54
5.1.7	Waste disposal	54
5.1.8	Off-site backup	54
5.2	Procedural Controls	54
5.2.1	Trusted roles	54
5.2.2	Number of persons required per task	54
5.2.3	Identification and authentication for each role	54
5.3	Personnel Controls	55
5.3.1	Background, qualifications, experience, and clearance requirements	55
5.3.2	Background check procedures	55
5.3.3	Training requirements	56
5.3.4	Retraining frequency and requirements	56
5.3.5	Job rotation frequency and sequence	56
5.3.6	Sanctions for unauthorized actions	56
5.3.7	Contracting personnel requirements	56
5.3.8	Documentation supplied to personnel	56
6	TECHNICAL SECURITY CONTROLS	57
6.1	Key Pair Generation and Installation	57
6.1.1	Key pair generation	57
6.1.2	Private key delivery to entity	57
6.1.3	Public key delivery to certificate issuer	57
6.1.4	CA public key delivery to subscribers	57
6.1.5	Key sizes	58
6.1.6	Public key parameters generation	58
6.1.7	Parameter quality checking	58
6.1.8	Hardware/software key generation	58

6.1.9	Key usage purposes (as per X.509 v3 key usage field)	58
6.2	Private Key Protection	58
6.2.1	Standards for cryptographic module	60
6.2.2	Private key (n out of m) multi-person control	60
6.2.3	Private key escrow	60
6.2.4	Private key backup	60
6.2.5	Private key archival	61
6.2.6	Private key entry into cryptographic module	61
6.2.7	Method of activating private key	61
6.2.8	Method of deactivating private key	61
6.2.9	Method of destroying private key	61
6.3	Other Aspects of Key Pair Management	62
6.3.1	Public key archival	62
6.3.2	Usage periods for the public and private keys	62
6.4	Activation Data	62
6.4.1	Activation data generation and installation	62
6.4.2	Activation data protection	62
6.4.3	Other aspects of activation data	62
6.5	Computer Security Controls	63
6.5.1	Specific computer security technical requirements	63
6.5.2	Computer security rating	63
6.6	Life-Cycle Technical Controls	63
6.6.1	System development controls	63
6.6.2	Security management controls	63
6.6.3	Life cycle security ratings	63
6.7	Network Security Controls	64
6.8	Cryptographic Module Engineering Controls	64
7	CERTIFICATE AND CRL PROFILES	65
7.1	Certificate Profile	65
7.1.1	Version number	65
7.1.2	Certificate extensions	65
7.1.3	Algorithm object identifiers	67

<i>CONTENTS</i>	9
7.1.4 Name forms	68
7.1.5 Name constraints	70
7.1.6 Certificate policy Object Identifier	70
7.1.7 Usage of Policy Constraints extensions	70
7.1.8 Policy qualifier syntax and semantics	70
7.1.9 Processing semantics for the critical certificate policy .	70
7.2 CRL Profile	71
7.2.1 Version number	71
7.2.2 CRL and CRL Entry Extensions	71
8 SPECIFICATION ADMINISTRATION	73
8.1 Specification Change Procedures	73
8.2 Publication and Notification Policies	74
8.3 CPS Approval Procedures	74
A Revision History	75
B Compliance with Laws and Regulations	79
B.1 The Data Protection Act	79
B.1.1 Definitions	79
B.1.2 Preliminaries	80
B.1.3 Data	80
B.1.4 Consent	81
B.1.5 Processing	81
B.1.6 Purpose	82
B.1.7 Data Release	83
B.1.8 Data Maintenance	83
B.1.9 Data Retention	84
B.1.10 Data Termination	84

Chapter 1

INTRODUCTION

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

1.1 Overview

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

This document was issued on 3 July 2006. An update was issued 18 July 2006 which fixes the description of the CA certificate extensions, removing subject and issuer alternative names, and the netscape CA extension. Another update was issued on 23 July 2006 to permit robot proxies, and to permit optional object signing extensions in user certificates.

THIS DOCUMENT IS THE CHANGELOG VERSION BETWEEN
VERSIONS 1.2 AND 1.3. IT IS NOT ITSELF A VALID CP/CPS. IT
DOCUMENTS CHANGES BETWEEN THE VERSIONS.

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

1.1.1 General definitions

The document makes use of the following terms:

Activation data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share)
Authentication	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.
Certificate Policy (CP)	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.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

Certification Authority (CA)	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.
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.
<u>Robot</u>	<u>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.</u>
<u>Service</u>	<u>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.</u>

Signed Email	In this document, “Signed Email” means an email that satisfies all of the following: (1) it is <i>not encrypted</i> , (2) it has a valid signature, and (3) the certificate corresponding to the private key that generated the signature is a valid UK e-Science CA certificate, and (4) the Common Name of the certificate bears a reasonable relation to the sender address of the email <u>the sender address is the same as the one in the subject alternative name.</u>
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.

20 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	ChangeLog 1.2-1.3-3
Document date	3 July 2006
Updated	18 July 2006
Updated	23 July 2006
Effective from	4 August 2006 (if approved)

21 The document OID will be `{iso(1) identified-organization(3) dod(6)`
 22 `internet(1) private(4) enterprise(1) cclrc(11439) 1 escience(1)`
 23 `ca(1) cps(1) 7}`.

24 See also revision history in Appendix A.

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

28 1.3 Community and Applicability

29 1.3.1 Certification authorities

30 The e-Science CA ~~self-certifies its own certificate~~ is a subordinate CA under
 31 the e-Science Root CA. It does not issue certificates to subordinate CAs.

32 1.3.2 Registration authorities

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

39 cates.

40 **1.3.3 End entities (Subscribers)**

41 The e-Science CA issues certificates for e-Science activities funded by the UK
42 Research Councils. The CA will issue personal, and host, ~~server~~ service, and
43 robot certificates.

44 **1.3.4 Applicability**

45 Certificates issued are suitable for the following applications:

- 46 • SSL or GSI client (all certificates);
- 47 • SSL or GSI server (host and service certificates only);
- 48 • GSI service (service certificates only);
- 49 • Generating GSI proxies (all certificates ~~except robot certificates~~);

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

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

55 **1.4 Contact Details**

56 **1.4.1 Specification administration organisation**

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

58 **1.4.2 Contact person**

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

61 Dr Jens G Jensen
62 Rutherford Appleton Laboratory

63 Chilton
64 Didcot
65 Oxon
66 OX11 0QX
67 UK
68
69 Phone: +44 1 235 446104
70 Fax: +44 1 235 445945
71 Email: ca-manager@grid-support.ac.uk

72 **1.4.3 Person determining CPS suitability for the pol-**
73 **icy**

74 The person mentioned in 1.4.2.

75 Chapter 2

76 GENERAL PROVISIONS

77 2.1 Obligations

78 2.1.1 CA obligations

79 The CA must:

- 80 • publish a CP and a CPS, structured according to RFC2527, [CF99];
- 81 • ensure that operations and infrastructure conform to this CP/CPS;
- 82 • issue certificates to entitled Subscribers based on validated requests
83 from Registration Authorities;
- 84 • notify the Subscriber of the issuing of the certificate;
- 85 • ~~publish a list of the issued certificates;~~
- 86 • accept revocation requests according to the procedures outlined in this
87 document;
- 88 • authenticate entities requesting the revocation of a certificate;
- 89 • generate and publish Certificate Revocation Lists (CRL) as described
90 in the CPS;
- 91 • identify and publish a list of the services for which service certificates
92 are issued (cf. RFC1738 [BLMM94], section 4);
- 93 • identify and publish a list of the robots for which robot certificates are
94 issued (cf. sections 3.1.2 and 7.1.2);

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

97 The CA is also an RA. ~~For this purpose,~~The CA Manager appoints an is
98 ~~considered the~~ RA Manager for the CA and who must adhere ~~also~~ to the RA
99 Manager's obligations. Each CA Operator, when acting as an RA Operator,
100 must adhere also to RA Operators' obligations.

101 **2.1.2 RA obligations**

102 The RA Manager must:

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

118 The RA Operator must:

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

- 124 ● for both host and service certificates, verify that the Subscriber is the
125 *responsible system administrator* for the resource identified by the cer-
126 tificate, or authorised by the administrator to apply for a certificate;
- 127 ● for robot certificates, verify that the applicant has satisfied the robot
128 requirements (cf. sections 4.1 and 3.1.2));
- 129 ● check that additional location-specific requirements (if any) are fulfilled
130 (an RA may have more stringent requirements for verifying a request
131 than the minimum requirements set out in this policy document - in
132 that case, the RA’s web page should list these requirements);
- 133 ● comply with the DPA compliance statement set out in Appendix B.1,
134 and, in particular:
 - 135 – ask the Subscriber only for adequate and relevant information
136 necessary to validate the request according to this CP/CPS and
137 to additional RA-specific requirements, and
 - 138 – process any personal data given by the subscriber (regardless of its
139 adequacy or relevance) according to the DPA compliance statement
140 in Appendix B.1;
- 141 ● provide information to the Subscriber on how to properly maintain a
142 certificate and the corresponding private key;
- 143 ● check that the information provided in the certificate request is correct
144 as described in section 3.1.9;
- 145 ● sign Subscriber’s request when and only when all conditions for issuing
146 a certificate to the Subscriber are fulfilled;
- 147 ● Request revocation of a Subscriber’s certificate when and only when
148 the RA Operator is aware that (1) the circumstances for revocation
149 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

150 2.1.3 Subscriber obligations

151 Subscribers must:

- 152 ● ~~read~~ and adhere to the procedures published in this document;
- 153 ● generate a key pair using a trustworthy method;

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

178 It is the Subscriber's obligation to provide to the RA Operator the information
179 required by the RA Operator to validate the request. This information may
180 depend on the type of request. However, the RA operator must ask only for
181 relevant and adequate information to validate the request (cf. Appendix B.1)
182 and the Subscriber is under no obligation to provide further information.

183 By submitting such information to the RA Operator, the Subscriber shall
184 be considered to have consented that all the information may be processed by
185 the CA and RA according to the DPA compliance statements in Appendix B.1.

186 **2.1.4 Relying party obligations**

187 A Relying Party should accept the Subscriber's certificate for authentication
188 purposes if:

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

197 The Relying Party must:

- 198 • use the Subscriber's certificates for the permitted purposes only;
- 199 • use for authorisation purposes either
 - 200 – the Subscriber's full DN; or
 - 201 – only the common root (`/C=UK/O=eScienceCA`); or
 - 202 – for host or service certificates, the CN or parts of the CN; or
 - 203 – for robot certificates, the Robot CN (see section 3.1.2 and 7.1.2).

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

207 **2.1.5 Repository obligations**

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

2.2 Liability

2.2.1 CA liability

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

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

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

2.2.2 RA liability

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

2.3 Financial Responsibility

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

2.3.1 Indemnification by relying parties

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

238 **2.3.3 Administrative processes**

239 No stipulation.

240 **2.4 Interpretation and Enforcement**

241 **2.4.1 Governing law**

242 Interpretation of this policy is according to UK Law. This policy is governed
243 by, and is to be construed in accordance with, English law. The English
244 Courts will have exclusive jurisdiction to deal with any dispute which has
245 arisen, or may arise out of, or in connection with, this policy.

246 **2.4.2 Severability, survival, merger, notice**

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

257 In the event that the CA ceases operation, all Subscribers, sponsoring
258 organisations, RAs, and Relying Parties will be promptly notified of the
259 termination.

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

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

264 **2.4.3 Dispute resolution procedures**

265 No stipulation.

266 **2.5 Fees**

267 **2.5.1 Certificate issuance or renewal fees**

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

270 **2.5.2 Certificate access fees**

271 ~~No fees are charged for certificate access.~~

272 No stipulation.

273 **2.5.3 Revocation or status information access fees**

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

276 **2.5.4 Fees for other services such as policy information**

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

280 **2.5.5 Refund policy**

281 No stipulation.

282 **2.6 Publication and Repositories**

283 **2.6.1 Publication of CA information**

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

- 285 • The e-Science CA's certificate;
- 286 • ~~Certificates issued;~~
- 287 • Certificate Revocation Lists;

- 288 • A copy of the most recent version of this CP/CPS and all previous
289 versions since 0.7;
- 290 • A changelog version of each CP/CPS comparing it to the previous
291 (except 0.7 which was the first public version).
- 292 • Other relevant information.

293 2.6.2 Frequency of publication

- 294 • ~~Certificates will be published as soon as they are issued.~~
- 295 • CRLs will be published as described in 4.4.9.
- 296 • This CP/CPS will be published whenever it is updated.

297 2.6.3 Access controls

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

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

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

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

- 307 • a rekey of the same certificate,
- 308 • host or service certificates,
- 309 • robot certificates.

310 RA Operators and CA Operators must both authenticate using valid
311 certificates to be able to access the RA Operator interface and CA Operator
312 interface, respectively.

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

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

321 **2.6.4 Repositories**

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

323 **2.7 Compliance Audit**

324 **2.7.1 Frequency of entity compliance audit**

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

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

330 **2.7.2 Identity/qualifications of auditor**

331 No stipulation.

332 **2.7.3 Auditor's relationship to audited party**

333 An external audit can be ~~performed~~ requested by any UK government depart-
334 ment or UK academic institution, or peer CA, or major relying Grid. The
335 auditor can be chosen by the requestor but the CA may require evidence of
336 auditor's qualifications. The CA reserves the right to impose confidentiality
337 restrictions upon the auditor, for both security and DPA reasons.

338 **2.7.4 Topics covered by audit**

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

341 **2.7.5 Actions taken as a result of deficiency**

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

344 **2.7.6 Communication of results**

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

347 **2.8 Confidentiality**

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

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

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

360 **2.8.1 Types of information to be kept confidential**

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

365 **2.8.2 Types of information not considered confidential**

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

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

371 **2.8.3 Disclosure of certificate revocation/suspension in-** 372 **formation**

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

375 **2.8.4 Release to law enforcement officials**

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

379 **2.8.5 Release as part of civil discovery**

380 No stipulation.

381 **2.8.6 Disclosure upon owner's request**

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

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

391 **2.8.7 Other information release circumstances**

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

394 **2.9 Intellectual Property Rights**

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

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

399 Section 2.8 contains text derived from, or copied from, the UK Department
400 of Trade and Industry (DTI) supplementary example agreements from the
401 Lambert Working Group on Intellectual Property, and from the DTI Office of
402 Science and Technology LINK CBI/AURIL model collaboration agreement.

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

406 This document typeset with L^AT_EX.

407 Chapter 3

408 IDENTIFICATION AND 409 AUTHENTICATION

410 3.1 Initial Registration

411 3.1.1 Types of names

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

415 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.

<u>Robot</u>	<u>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.</u>
--------------	--

416

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

420 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

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

423 Robot certificate names satisfy the same constraints as personal certificates
 424 except that the additional CN, identifying the certificate as a robot certificate
 425 and the type of the robot, begins with 'Robot:' (including the semicolon,
 426 which cannot occur in other types of certificates). This string is followed by
 427 the *type* of the robot, which is always a string consisting of letters. Additional
 428 text may be contained in the CN for disambiguation purposes, in which case
 429 a space separates the type from the disambiguation string.

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

431 '0' - '9', 'a' - 'z', 'A' - 'Z', '-', '.'

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

435 Email address in server and service certificates must be structured ac-
 436 cording to RFC822 and must be in the "addr-spec" format as defined in
 437 RFC822. The maximal length of an email address is 128 characters. Email
 438 addresses must be encoded as `IA5String` in the name but must not con-
 439 tain control characters or delete. For personal certificates, email addresses
 440 in subject alternative name must be included as `rfc822Name` and satisfy the
 441 same constraints.

442 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 (~~other than the root certificate~~), 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].

477 **3.1.3 Rules for interpreting various name forms**

478 No stipulation.

479 **3.1.4 Uniqueness of names**

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

488 The e-Science CA will ~~make reasonable attempts to~~ ensure that a DN
489 is not reused. If a person requests a certificate with the same DN as an
490 existing certificate (regardless of the status of this certificate) and the request
491 is not a renewal or rekey, the RA Operator will consult the original Personal
492 Information to ensure that the Subscriber is the same as the person who was
493 identified in the original certificate. If this identity cannot be established,
494 the DN will never be reused.

495 **3.1.5 Name claim dispute resolution procedure**

496 No stipulation.

497 **3.1.6 Recognition, authentication and role of trade-** 498 **marks**

499 No stipulation.

500 **3.1.7 Method to prove possession of private key**

501 ~~No stipulation.~~

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

504 3.1.8 Authentication of organisation identity

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

508 There is no verification of individuals' organisation identity.

509 3.1.9 Authentication of individual identity

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

512 In either case the Subscriber selects which RA is to carry out the identi-
 513 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).
<u>Robot</u>	<u>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).</u>

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

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

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

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

527 **3.2 Routine Re-key**

528 ~~No stipulation.~~

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

531 **3.3 Re-key After Revocation**

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

534 **3.4 Revocation Request**

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

539 Authenticated certificate revocation requests may be made by

- 540 • The RA using:
 - 541 – Signed Email to the CA Manager;
 - 542 – Other secure method, as specified in the RA Operator's procedure.

- 543 • The Subscriber by:
- 544 – Mailing the CA manager directly by Signed Email.

Chapter 4

OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Procedures are different if the Subscriber is a person or a server. In every case The Subscriber has to generate his/her own key pair. The minimum key length is 1024 bits. Personal and robot certificates must not be shared; server certificates must be linked to a single network entity. Maximal lifetime of a certificate is ~~one year~~ 395 days. The default validity period is ~~one year~~ the maximum.

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

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

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

- a rekey of the same certificate,
- host or service certificates,
- robot certificates.

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

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

568 4.2 Certificate Issuance

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

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

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

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

581 If the authentication is unsuccessful, the certificate is not issued and an
582 e-mail with the reason is sent to the Subscriber or the Subscriber is otherwise
583 notified by CA or RA staff. In particular, the CA or RA may delete a request
584 if the Subscriber has made no attempt to authenticate him- or herself within
585 30 days of submitting the request.

586 All issued certificates are issued under the CP/CPS valid at the time of
587 issuance.

588 4.3 Certificate Acceptance

589 No stipulation.

590 4.4 Certificate Suspension and Revocation

591 4.4.1 Circumstances for revocation

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

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

- 598 3. the information in the Subscriber's certificate is wrong or inaccurate,
599 or suspected to be wrong or inaccurate;
- 600 4. the Subscriber violates his/her obligations.

601 It is worth noting that items 1 and 4 above may entail a revocation of *all*
602 the Subscriber's certificates; in the case of item 4, depending on the nature
603 of the violation. The CA may provide facilities for the Subscriber to "hand
604 over" a host or service certificate to a successor, if the reason for revocation
605 is reason 1, provided this can be done without invalidating the information
606 in the certificate. In this case, the RA will verify that the successor is a
607 responsible administrator of the host or service in question. Robot certificates
608 tied to the Subscriber's identity will always be revoked.

609 4.4.2 Who can request revocation

610 A certificate revocation can be requested by:

- 611 • The Registration Authority which authenticated the holder of the cer-
612 tificate;
- 613 • the holder of the certificate;
- 614 • any person presenting proof of knowledge that the Subscriber's private
615 key has been compromised or that the Subscriber's data have changed.

616 4.4.3 Procedure for revocation request

617 A revocation request is accepted if:

- 618 • The revocation request is signed with the key corresponding to certifi-
619 cate whose revocation is requested; or,
- 620 • The revocation request is signed by the RA who originally approved
621 the certificate request.

622 Any other revocation request is accepted only if the entity requesting the
623 revocation is properly authenticated.

624 **4.4.4 Revocation request grace period**

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

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

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

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

635 **4.4.5 Circumstances for suspension**

636 The CA does not offer suspension services.

637 **4.4.6 Who can request suspension**

638 No stipulation.

639 **4.4.7 Procedure for suspension request**

640 No stipulation.

641 **4.4.8 Limits on suspension period**

642 No stipulation.

643 **4.4.9 CRL issuance frequency**

644 CRLs are updated and re-issued within one hour after every approved cer-
645 tificate revocation, but ~~or~~ at least once every week.

646 **4.4.10 CRL checking requirements**

647 No stipulation.

648 **4.4.11 On-line revocation/status checking availability**

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

650 **4.4.12 On-line revocation checking requirements**

651 No stipulation.

652 **4.4.13 Other forms of revocation advertisements avail-**
653 **able**

654 No stipulation.

655 **4.4.14 Checking requirements for other forms of revo-**
656 **cation advertisements**

657 No stipulation.

658 **4.4.15 Special requirements re key compromise**

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

663 **4.5 Security Audit Procedures**

664 **4.5.1 Types of event recorded**

665 The following events are recorded:

- 666 • certification requests;
- 667 • issued certificates;
- 668 • requests for revocation;
- 669 • issued CRLs;
- 670 • login/logout/reboot of the signing machine.

671 **4.5.2 Frequency of processing log**

672 No stipulation.

673 **4.5.3 Retention period for audit log**

674 The minimum retention period is 3 years.

675 **4.5.4 Protection of audit log**

676 No stipulation.

677 **4.5.5 Audit log backup procedures**

678 No stipulation.

679 **4.5.6 Audit collection system (internal vs external)**

680 No stipulation.

681 **4.5.7 Notification to event-causing subject**

682 No stipulation.

683 **4.5.8 Vulnerability assessments**

684 No stipulation.

685 **4.6 Records Archival**

686 **4.6.1 Types of event recorded**

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

- 688 • certification requests;
- 689 • issued certificates;

- 690 • requests for revocation;
- 691 • issued CRLs;
- 692 • all e-mail messages received by the CA (not the confirmation messages
693 sent to the Subscribers);
- 694 • all e-mail messages sent by the CA;
- 695 • all documents appointing CA and RA Staff.

696 Each RA must log the following:

- 697 • for each approved request, how it was approved;
- 698 • for each rejected request, why it was rejected;
- 699 • for each approved revocation request, the reason for revocation;
- 700 • for each rejected revocation request, the reason for revocation and the
701 reason the request was rejected.

702 **4.6.2 Retention period for archive**

703 The minimum retention period is 3 years.

704 **4.6.3 Protection of archive**

705 No stipulation.

706 **4.6.4 Archive backup procedures**

707 No stipulation.

708 **4.6.5 Requirements for time-stamping of records**

709 No stipulation.

710 **4.6.6 Archive collection system (internal or external)**

711 No stipulation.

712 **4.6.7 Procedures to obtain and verify archive informa-** 713 **tion**

714 No stipulation.

715 **4.7 Key Changeover**

716 The CA will generate a new ~~root~~ key pair and obtain a new CA certificate
717 from the Root one year and 30 days (the maximal lifetime of a Subscriber's
718 certificate) before the expiry of the CA certificate. In the final year the CA's
719 old certificate will be available for validation purposes only, whereas new
720 certificates and CRLs will be signed with the new CA key.

721 **4.8 Compromise and Disaster Recovery**

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

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

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

730 **4.8.1 Computing resources, software, and/or data are** 731 **corrupted**

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

733 **4.8.2 Entity public key is revoked**

734 No stipulation.

735 **4.8.3 Entity key is compromised**

736 No stipulation.

737 **4.8.4 Secure facility after a natural or other type of**
738 **disaster**

739 No stipulation.

740 **4.9 CA Termination**

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

- 742 • inform the Registration Authorities, Subscribers, Relying Parties, and
743 cross-certifying CAs of which the CA is aware;
- 744 • make information of its termination widely available;
- 745 • stop issuing certificates.

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

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

756 Chapter 5

757 PHYSICAL, PROCEDURAL, 758 AND PERSONNEL 759 SECURITY CONTROLS

760 5.1 Physical Controls

761 5.1.1 Site location and construction

762 No stipulation.

763 5.1.2 Physical access

764 The CA operates in a controlled environment, where access is restricted to
765 authorised people and logged. The signing machine is connected to the online
766 machine via a private and monitored network. The signing machine has a
767 the private key stored in an HSM with certification to FIPS-140-2 Level 3.
768 is kept locked in a safe and the private key is locked in a different safe.

769 5.1.3 Power and air conditioning

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

773 ~~The signing machine is switched off between signing operations. The~~
774 ~~machine operates in an air conditioned environment.~~

775 **5.1.4 Water exposures**

776 No stipulation.

777 **5.1.5 Fire prevention and protection**

778 No stipulation.

779 **5.1.6 Media storage**

780 No stipulation.

781 **5.1.7 Waste disposal**

782 No stipulation.

783 **5.1.8 Off-site backup**

784 No stipulation.

785 **5.2 Procedural Controls**

786 **5.2.1 Trusted roles**

787 No stipulation.

788 **5.2.2 Number of persons required per task**

789 No stipulation.

790 **5.2.3 Identification and authentication for each role**

791 No stipulation.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

- The CA Manager must be a paid employee of CCLRC and shall be appointed in writing by the CCLRC Director of e-Science who may at his/her discretion revoke the appointment with no prior notice given.
- The CA Operators must be paid employees of CCLRC and will be appointed by the CA Manager.
- The RA Manager must be a paid employee of the Physical Organisation hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that physical organisation. The RA Manager must be a member of that Department. The OU field of the RA Operator's certificate identifies the Physical Organisation. and 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.

825 **5.3.3 Training requirements**

826 No stipulation.

827 **5.3.4 Retraining frequency and requirements**

828 No stipulation.

829 **5.3.5 Job rotation frequency and sequence**

830 No stipulation.

831 **5.3.6 Sanctions for unauthorized actions**

832 In the event of unauthorised actions, abuse of authority or unauthorised use
833 of entity systems by the CA or RA Operators, the CA manager may revoke
834 the privileges concerned.

835 **5.3.7 Contracting personnel requirements**

836 No stipulation.

837 **5.3.8 Documentation supplied to personnel**

- 838 • It is the responsibility of the CA Manager to provide the CA Operators
839 with a copy of the “e-Science CA Operator’s Procedure”.
- 840 • It is the responsibility of the CA Manager to provide the RA Manager
841 with a copy of the “e-Science RA Manager’s Procedure”.
- 842 • It is the responsibility of the RA Manager to provide the RA Operator
843 with a copy of the “e-Science RA Operator’s Procedure”.

844 Chapter 6

845 TECHNICAL SECURITY 846 CONTROLS

847 6.1 Key Pair Generation and Installation

848 6.1.1 Key pair generation

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

851 6.1.2 Private key delivery to entity

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

854 6.1.3 Public key delivery to certificate issuer

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

857 6.1.4 CA public key delivery to subscribers

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

860 **6.1.5 Key sizes**

861 Keys of length less than 1024 bits are not accepted. The CA key is of length
862 2048 bits.

863 **6.1.6 Public key parameters generation**

864 No stipulation.

865 **6.1.7 Parameter quality checking**

866 No stipulation.

867 **6.1.8 Hardware/software key generation**

868 ~~No stipulation.~~ If the private key is protected by a hardware token, it must
869 be generated on that token.

870 **6.1.9 Key usage purposes (as per X.509 v3 key usage** 871 **field)**

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

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

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

877 **6.2 Private Key Protection**

878 The following table summarises how Subscribers' private keys must be protected,
879 depending on the type and use of the corresponding certificate. Other
880 protection methods are permissible if they are equivalent or stronger.

<u>Type</u>	<u>Personal</u>	<u>Host</u>	<u>Service</u>	<u>Robot</u>
<u>file system, user only</u>			■	
<u>file system, root only</u>		■	■	
<u>file system, encrypted, Subscriber only</u>	■	■	■	
881 <u>key token</u>	■	■	■	■

882 The protections above are to be interpreted as follows:

883 • **File system, user only:**

- 884 – The private key is protected by file system access control, in such
- 885 a way that only its primary user can access it.
- 886 – The primary user need not be the same as the Subscriber (who is
- 887 responsible for the certificate), but must have been granted access
- 888 by the Subscriber.
- 889 – The Subscriber must be responsible for the host in which the
- 890 credentials are installed, and must be responsible for granting
- 891 and revoking privileged access (who can potentially bypass file
- 892 protection) to the filesystem to others.

893 • **File system, root only:**

- 894 – The private key is protected by file system access control, in such
- 895 a way that only privileged users can access it.
- 896 – The key may be stored in a system-user account, provided no
- 897 non-privileged users can read the key from that account.
- 898 – The Subscriber must be responsible for the host in which the
- 899 credentials are installed, and must be responsible for granting
- 900 and revoking privileged access (who can potentially bypass file
- 901 protection) to the filesystem to other users.

902 • **File system, encrypted, Subscriber only:**

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

- 906 – The symmetric encryption key should be generated from a Strong
907 passphrase, using PKCS#5 version 2.0 or later; if another encryption
908 method is used, the other method must be equivalent or stronger.
- 909 – Users should make best endeavours that the encrypted key is not
910 copied around or stored on shared filesystems.
- 911 • Key token:
- 912 – The key token protecting the private key must satisfy the constraints
913 of section 6.2.1.

914 **6.2.1 Standards for cryptographic module**

915 ~~No stipulation.~~ The CA's private key is protected by an HSM certified to
916 FIPS 140-2 Level 3.

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

920 **6.2.2 Private key (n out of m) multi-person control**

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

923 Backup copies of the CA's private key is under (3 out of 5) ~~(2 out of 3)~~
924 multi-person control (as well as locked in a safe as described in 6.2.4).

925 **6.2.3 Private key escrow**

926 Private keys must not be escrowed.

927 **6.2.4 Private key backup**

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

932 The private key of the CA is encrypted within the HSM using keys held
933 on secure key tokens (see also section 6.2.2). The backup copy can thus be
934 backed up normally with the rest of the filesystem and databases (but of

935 course with access controls on the backups).

936 **6.2.5 Private key archival**

937 No stipulation.

938 **6.2.6 Private key entry into cryptographic module**

939 ~~No stipulation.~~

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

942 A Subscriber's private key, when protected by a key token, must be
943 generated in that token.

944 **6.2.7 Method of activating private key**

945 ~~The CA private key is activated by a pass phrase which, for emergencies, is~~
946 ~~kept in a sealed envelope in a safe. The safe which contains the pass phrase~~
947 ~~does not contain any copy of the private key.~~

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

951 **6.2.8 Method of deactivating private key**

952 ~~No stipulation.~~

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

956 **6.2.9 Method of destroying private key**

957 No stipulation.

958 **6.3 Other Aspects of Key Pair Management**

959 **6.3.1 Public key archival**

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

962 **6.3.2 Usage periods for the public and private keys**

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

965 **6.4 Activation Data**

966 ~~The CA private key is protected by a Strong Pass phrase.~~

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

971 **6.4.1 Activation data generation and installation**

972 No stipulation.

973 **6.4.2 Activation data protection**

974 ~~All CA Operators know the Activation Data for the CA private key. No~~
975 ~~other person knows the Activation Data. However, the Activation Data for~~
976 ~~the CA private key is also kept in a sealed envelope in a safe in a separate~~
977 ~~location from the safes containing the private key and its backup copies.~~

978 See section 6.4.

979 **6.4.3 Other aspects of activation data**

980 No stipulation.

981 **6.5 Computer Security Controls**

982 **6.5.1 Specific computer security technical requirements**

983 The CA server and all other machines on the CA's private subnet, including
984 the signing machine, are secured as follows includes the following functionality:

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

990 The CA has a security document describing in detail the security infrastructure
991 and logging. For security reasons, this document is available only to CA staff,
992 relevant site operational security staff, and auditors.

993 **6.5.2 Computer security rating**

994 No stipulation.

995 **6.6 Life-Cycle Technical Controls**

996 **6.6.1 System development controls**

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

999 **6.6.2 Security management controls**

1000 No stipulation.

1001 **6.6.3 Life cycle security ratings**

1002 No stipulation.

1003 **6.7 Network Security Controls**

1004 Certificates are generated on a machine ~~not~~ connected to ~~any kind of a~~
1005 private, dedicated, network, located in a secure environment and managed
1006 by a suitably trained person. All ~~The public machines are~~ is protected by a
1007 suitably configured firewalls.

1008 **6.8 Cryptographic Module Engineering Con-** 1009 **trols**

1010 No stipulation.

1011 Chapter 7

1012 CERTIFICATE AND CRL 1013 PROFILES

1014 7.1 Certificate Profile

1015 7.1.1 Version number

1016 X.509.v3

1017 7.1.2 Certificate extensions

1018 Host and service certificates have the same extensions.

1019 Robot certificates can have different extensions, depending on the type
1020 and use of the robot. Each type of robot and its certificate profile is documented
1021 in detail in a separate document available from the CA's web site.

1022 In any case, the extensions accorded to robot certificates is a (not necessarily
1023 proper) subset of those accorded to Personal certificates, *except* that:

- 1024 • robot certificates may have extended key usage set;
- 1025 • robot certificates have a *second* OID in their PolicyInformation, namely,
1026 that of the robot 1SCP under which they are issued (that of the CP/CPS
1027 under which they are issued is the first).

1028 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, issuer
<u>Subject Alternative Name</u> (personal/robot)	<u>Subject's personal email address</u>
Subject Alternative Name (server/service)	Server's Fully Qualified Domain Name
Issuer Alternative Name	CA email
CRL Distribution Points	<u>HTTP URL of CRL</u>
Netscape Cert Type	Personal, <u>Robot</u> : SSL Client, S/MIME Personal: (optionally) object signing Server, service: SSL Client, SSL Server
Netscape Comment	"UK e-Science <u>XXX</u> Certificate" where "XXX" is "User", "Host", "Service", or "Robot".
Netscape CA Revocation URL	<u>HTTP URL of CRL</u>
Netscape Revocation URL	<u>HTTP URL of CRL</u>

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

1029 The CA operator certificate (see section 3.1.2) has the same extensions as a
 1030 user certificate. It always has the Netscape Object Signing extension set.

1031 **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, issuer
Subject—Alternative Name	CA email
Issuer—Alternative Name	CA email
CRL—Distribution Points	http://ca.grid-support.ac.uk/cgi-bin/importCRL
Netscape Cert Type	SSL CA, S/MIME CA
Signature Algorithm	sha1WithRSAEncryption

1032 7.1.3 Algorithm object identifiers

1033 No stipulation.

1034 **7.1.4 Name forms**1035 **CA certificate**

1036 Issuer:

1037 /C=UK/O=eScienceRoot/OU=Authority/L=Root/CN=CA

1038 Subject:

1039 /C=UK/O=eScienceCA/OU=Authority/CN=CA

1040 Note that the subject has /C=UK/O=eScienceCA/* to avoid having the
 1041 root sign in the same namespace as the CA described in this CP/CPS.

1042 **End Entity Certificate**1043 Issuer: is the CA's subject DN.

1044 Subject: The subject field contains the Distinguished Name of the entity
 1045 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 object-signing <u>robot</u> : 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).
<u>CommonName</u>	<u>Robots have an additional CN of the form Robot: type.</u>

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

1046 Important notes:

- 1047 • The DN of EEs is preserved across the CA certificate rollover.
- 1048 • The CN in a personal certificate may contain additional text string,
1049 as described in section 3.1.2. Likewise, the additional robot CN may
1050 contain an additional text string, as described in the same section.

1051 The name of the special CA operator (see section 3.1.2) certificate is

1052 /C=UK/O=eScience/OU=Authority/L=CLRC/CN=ca-operator

1053 The email address in host and service certificates must be that of a one
1054 or more ~~person~~ people responsible for the server in question, and need not be
1055 a personal address. Host certificates should not have “host” as a service, i.e.
1056 they should have CN=host.univ.ac.uk and not CN=host/host.univ.ac.uk
1057 if they are used with non-Globus servers.

1058 The CA will issue certificates for a given service if and only if:

- 1059 • the service has been defined by IANA [IAN]; or
- 1060 • The CA Manager has approved the service.

1061 It is the responsibility of the CA Manager to define the non-IANA services
1062 allowed by the CA. For each service, the CA Manager must provide

- 1063 • the name of the service,
- 1064 • the default port number,
- 1065 • a short description of the service,
- 1066 • a reference URI.

1067 The CA Manager must ensure that services are unique in name.

1068 It is the responsibility of the CA Manager to define the robot types
1069 supported by the CA. For each robot type, the CA Manager must provide

- 1070 • the name of the robot type (as in CN=Robot: *type*);

- 1071 • The exact profile of the robot (extensions);
- 1072 • Purposes for which the robot certificate is to be used;
- 1073 • Purposes for which using the robot certificate is explicitly forbidden, if
1074 any;
- 1075 • Additional qualifications a requestor must have and prove to an RA in
1076 order to successfully obtain a robot certificate, if any.

1077 **7.1.5 Name constraints**

1078 No stipulation¹.

1079 **7.1.6 Certificate policy Object Identifier**

1080 ~~No stipulation.~~

1081 Certificates contain in the PolicyInformation extension the policyIdentifier
1082 containing the OID of the CP/CPS under which they were issued. Additionally,
1083 robot certificates contain an 1SCP robot OID.

1084 **7.1.7 Usage of Policy Constraints extensions**

1085 No stipulation.

1086 **7.1.8 Policy qualifier syntax and semantics**

1087 No stipulation.

1088 **7.1.9 Processing semantics for the critical certificate** 1089 **policy**

1090 No stipulation.

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

1091 **7.2 CRL Profile**

1092 **7.2.1 Version number**

1093 X.509.v1: Version 1 is required for compatibility with Netscape Communi-
1094 cator.

1095 **7.2.2 CRL and CRL Entry Extensions**

1096 No stipulation.

1097 Chapter 8

1098 SPECIFICATION 1099 ADMINISTRATION

1100 8.1 Specification Change Procedures

1101 We distinguish between different types of modifications to the CP/CPS:

1102 *Editorial updates:* editorial changes to the CPS, including replacing fields
1103 with “No stipulation”, as long as they do not affect procedure or compromise
1104 security. These changes are announced on the CA web site but no advance
1105 warning will be given.

1106 *Procedure updates:* minor changes to the CPS that do not compromise secu-
1107 rity in any way. E.g. changes to the verification or issuing procedure that
1108 do not affect security. Subscribers and relying parties will not be warned of
1109 such changes in advance but RAs will be given at least one week’s notice of
1110 changes that affect their procedures.

1111 *Technical updates:* e.g. changes to the extensions in the issued certificates.
1112 Such changes will be announced on the CA web site and on appropriate
1113 mailing lists at least 14 days in advance.

1114 *Security updates:* changes that affect the security, e.g. changes to the minimal
1115 requirements for verifying requests, or changing the key sizes. These changes
1116 will be announced at least 30 days in advance on the CA web site, and to
1117 appropriate mailing lists, including the EU Grid PMA mailing list. However,
1118 urgent security fixes may be carried out without advance warning and then
1119 documented in the CPS. These will be announced in the same manner.

1120 *Policy updates:* e.g. changes to the namespace, or introducing subordinate
1121 CAs. A proposal will be announced at least 30 days in advance on the CA

1122 web site and appropriate mailing lists.

1123 *Termination:* A scheduled termination of the CA is announced on the CA
1124 web site and appropriate mailing lists at least 60 days in advance.

1125 **8.2 Publication and Notification Policies**

1126 This CP/CPS is available at [CAW]. All changes are announced on the CA
1127 web site and a changelog is available. In addition, changes are announced to
1128 appropriate mailing lists, depending on the type of change, as described in
1129 section 8.1.

1130 There is a mailing list for RA Managers and Operators. Only subscribers
1131 can post to the mailing list. Only subscribers can read the archives.

1132 **8.3 CPS Approval Procedures**

1133 No stipulation.

1134 Appendix A

1135 Revision History

1136

Version	OID	Date	Comments
0.1		4 September 2001	Initial unapproved release
0.3		30 January 2002	Andrew's changes
0.4		13 March 2002	Jens' changes
0.5		April/May 2002	Tim's changes
0.6		28 May 2002	draft version
0.7	1.1	17 July 2002	final draft
0.8	1.2	10 October 2002	Removed identification by telephone, made specification of host verification more precise, added missing RFC2527 entries.
0.9	1.3	31 March 2003	Update to request extensions. Describe renewal. Tightened up several parts, including Applicability, personal information stored, etc.
1.0	1.4	30 October 2003	
1.1	1.5	04 March 2005	Documented that we use SHA1 to sign. Documented CA upgrade, Data protection act, and some codifications of existing practice.
1.2	1.6	15 May 2005	
1.3	1.7	3 July 2006	CA rollover, signing key online, robots.

1137

1138 The OID in the table is the final two digits of the actual OID, as defined in
1139 section 1.2.

1140 Appendix B

1141 Compliance with Laws and 1142 Regulations

1143 The UK e-Science CA operates under ~~UK~~ English Law. See section 2.4.1.

1144 In the case an RA Operator or CA Operator cannot complete his or her
1145 operations without violating rules set forth in this Appendix, the Operator
1146 must not complete the operation and must notify the CA Manager, and, if
1147 applicable, his or her RA Manager.

1148 B.1 The Data Protection Act

1149 The Data Protection Act 1998 (DPA) [DPA00].

1150 B.1.1 Definitions

- 1151 • The *data controller* is the CA Manager, the person mentioned in 1.4.2.
- 1152 • The *data processor* is any RA Manager or Operator.
- 1153 • The *data subject* is a Subscriber requesting a certificate, or an RA
1154 Operator or a CA Operator being appointed as such by the CA.
- 1155 • *Data* is to be understood as defined in DPA section I.1.
- 1156 • *Processing Data* is to be understood as defined in DPA section I.1.
- 1157 • Throughout this Appendix, *Personal Data* means Data which is Per-
1158 sonal Data as defined in DPA section I.1 but which is not *Sensitive*
1159 *Personal Data* as defined in DPA section I.2.

- 1160 • *Personal Information* is defined in section 1.1.1 of this document. For
1161 the purposes of the DPA,
- 1162 – the photo id is considered Sensitive Personal Data;
- 1163 – all other parts of Personal Information are considered Personal
1164 Data.

1165 B.1.2 Preliminaries

1166 The *intent* of Processing Data by the UK e-Science CA is that minimal and
1167 adequate Personal Information is stored and Processed in order that the UK
1168 e-Science CA may operate according to the policy and practices described
1169 in this CP/CPS, including being an internationally approved medium level
1170 CA.

1171 B.1.3 Data

1172 The UK e-Science CA stores the following Data:

- 1173 1. The CA publishes on its web page, and may publish by other methods,
1174 the Subscriber's *certificate* and thus all information contained therein,
1175 including the Subscriber's name;
- 1176 2. The CA logs and stores all Subscriber and RA interactions with the
1177 CA's online service, in order to satisfy the requirements of sections 4.5
1178 and 4.6 of this CP/CPS;
- 1179 3. The RA Operator Processes Personal Information, and possibly other
1180 Data, as described in section B.1.5;
- 1181 4. The CA stores authorisation information about the RA Manager and
1182 Operators sufficient to convince the CA that the RA Manager and
1183 Operators satisfy the conditions of section 5.3.1 and that the CA has the
1184 RA Manager's assurance that the RA Operator will operate according
1185 to this CP/CPS;
- 1186 5. For host and service certificates, it may be necessary to obtain and store
1187 Personal Data that proves to the RA Operator's satisfaction that Sub-
1188 scriber is responsible system administrator for the resource for which
1189 the Subscriber requests a certificate, in accordance with sections 2.1.2,
1190 2.1.3, and 3.1.9;

1191 6. It may be necessary to obtain and store Personal Data to prove to the
1192 RA Operator's satisfaction that the Subscriber is entitled to a certifi-
1193 cate from the UK e-Science CA, cf. section 1.3.3.

1194 Notwithstanding the above, the Data Processed by the UK e-Science CA is
1195 subject to the following restrictions:

- 1196 • The UK e-Science CA must not Process or attempt to Process any
1197 Sensitive Personal Data *except* the photo id.
- 1198 • Personal Data and Sensitive Personal Data must be relevant and ade-
1199 quate for the purpose for which it is Processed.
- 1200 • The UK e-Science CA must Process Personal Information only as de-
1201 fined in this Appendix, and in accordance with the DPA.

1202 B.1.4 Consent

1203 By submitting Data to the online CA ([CAW]), the Subscriber is considered
1204 to have given consent that the submitted Data may be Processed by the
1205 e-Science CA (there is a notice to this effect on the web page). By present-
1206 ing Personal Information to the RA Operator, the Subscriber is deemed to
1207 have given consent that this information may be Processed according to the
1208 purposes described in this document, and stored according to the procedures
1209 described in this document (there is a notice to this effect on the web page).
1210 By applying for RA Operator or CA Operator status, the RA Operator or CA
1211 Operator is deemed to have consented that the CA can Process the Data as
1212 described below (there is a notice to this effect in the template appointment
1213 letters provided by the CA).

1214 B.1.5 Processing

1215 The CA permits that Personal Information is Processed as follows:

- 1216 1. The CA Operator or RA Operator obtains Personal Information or
1217 other Data from the Subscriber or from another Operator relevant and
1218 adequate for the purposes described below;
- 1219 2. A photocopy of the Personal Information is made for the purposes
1220 described below;

- 1221 3. The photocopy of Personal Information is subsequently accessed only
1222 for the purposes described below;
- 1223 4. Subscriber's email address is obtained and used only for the purposes
1224 described below;
- 1225 5. Relevant and adequate information is Processed to satisfy section 4.5
1226 of this CP/CPS in accordance with sections 4.5 and 4.6.

1227 **B.1.6 Purpose**

1228 The UK e-Science CA Processes Personal Information for the following pur-
1229 poses:

- 1230 1. Identification of a Subscriber;
- 1231 2. Subsequent auditing of the Identification process, for the case where the
1232 UK e-Science CA must prove the link from the DN to the Subscriber's
1233 real identity;
- 1234 3. Release of Personal Information under the circumstances described in
1235 section 2.8 and according to the procedures described in the same sec-
1236 tion;
- 1237 4. To maintain the uniqueness of the DN to the extent described in sec-
1238 tion 3.1.4;
- 1239 5. For RA and CA Operators, to check to the CA Manager's satisfaction
1240 that the RA or CA Operator is duly authorised by appointment letter
1241 to operate according to this CP/CPS and that the RA Manager and
1242 Operator satisfy the conditions described in section 5.3.1;
- 1243 6. Adequate Personal Information is Processed to satisfy the auditing re-
1244 quirements set forth in sections 2.7, 4.5 and 4.6 of this CP/CPS;
- 1245 7. Email address is used only to notify the Subscriber that:
- 1246 • A new certificate has been issued to the Subscriber;
 - 1247 • A certificate held by the Subscriber is about to expire.

1248 Data may be used for statistical purposes

- 1249 • only with the Data Controller's permission; and

- 1250 • if there is reasonable cause; and
- 1251 • if the published information contain neither Personal Data nor Sensitive
1252 Personal Data, and no Personal Data or Sensitive Personal Data can
1253 be derived from it; and
- 1254 • the Processing associated with and required for statistical purposes are
1255 done in accordance with the DPA section 33.

1256 Any other use of Personal Information is explicitly forbidden.

1257 **B.1.7 Data Release**

1258 Circumstances requiring Processing of Personal Information include, but are
1259 not necessarily limited to, the following cases:

- 1260 1. A CA Manager or Operator is considered to have breached CA Obli-
1261 gations (section 2.1.1);
- 1262 2. An RA Manager or Operator is considered to have breached RA Obli-
1263 gations (section 2.1.2);
- 1264 3. A Subscriber is considered to have breached Subscriber's Obligations
1265 (section 2.1.3);
- 1266 4. Release of information as described in section 2.8, including any release
1267 required by UK law;
- 1268 5. Release of information as required for auditing purposes, including com-
1269 pliance audit as described in section 2.7.

1270 In each case, the UK e-Science CA shall ensure that only the adequate and
1271 relevant information is released and that the information is Processed law-
1272 fully and in accordance with the rules of sections B.1.5 and B.1.6, and in
1273 accordance with the DPA.

1274 **B.1.8 Data Maintenance**

1275 There is no requirement for keeping Personal Information Processed by the
1276 RA up to date, except to the extent required to satisfy the RA Operator
1277 that the information mentioned in 5 and 6 in section B.1.3 is still valid if and
1278 when certificates that required this information prior to their approval are
1279 being renewed.

1280 It is the RA Manager's responsibility to ensure that the Data Processed
1281 by the CA concerning his or her RA or any Manager or Operator associated
1282 with that RA is kept up to date, and inform the CA of any update.

1283 **B.1.9 Data Retention**

1284 Personal Information shall be kept by the UK e-Science CA for as long as is
1285 necessary:

- 1286 1. Personal Information used to obtain a personal certificate with a certain
1287 DN shall be kept for as long as the Subscriber has a valid certificate
1288 with this DN, including renewals of the certificate, and for a period
1289 beyond the expiry or revocation of the latest certificate held by the
1290 Subscriber necessary to satisfy the retention requirements described in
1291 section 4.6;
- 1292 2. Data used to obtain a host or service certificate shall be kept for as
1293 long as the Subscriber is responsible administrator for the resource for
1294 which the certificate was obtained, and for a period beyond the expiry
1295 or revocation of the latest certificate held by the Subscriber, or beyond
1296 the administrator rights being passed on to someone else, necessary to
1297 satisfy the retention requirements described in section 4.6.
- 1298 3. Data used by the CA Manager to authorise RA Managers and Op-
1299 erators must be kept for a period beyond the termination of the RA
1300 necessary to satisfy the requirements described in section 4.6. For the
1301 termination of the CA, the conditions in sections 4.6.2 and 4.9 apply.

1302 It is the responsibility of the RA Manager to ensure that appropriate techni-
1303 cal and organisational measures are taken against unlawful or unauthorised
1304 Processing of Data held by the RA. It is the responsibility of the CA Manager
1305 to ensure that appropriate technical and organisational measures are taken
1306 against unlawful or unauthorised Processing of Data held by the CA.

1307 **B.1.10 Data Termination**

1308 It is the responsibility of the RA Manager to ensure that Personal Information
1309 held and Processed by the RA is adequately destroyed by the end of the
1310 retention period. It is the responsibility of the CA Manager to ensure that
1311 Personal Information held and Processed by the CA is adequately destroyed
1312 by the end of the retention period.

1313 Bibliography

- 1314 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate
1315 policy model. [http://www.gridforum.org/2_SEC/pdf/Draft-](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf)
1316 [GGF-CP-06.pdf](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf), September 2001.
- 1317 [BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform resource
1318 locators. <http://www.rfc-editor.org/rfc/rfc1738.txt>, December
1319 1994.
- 1320 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 1321 [Cec01] R. Cecchini. INFN CA CP/CPS. [http://security.fi.infn.it/CA/-](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf)
1322 [CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 1323 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-
1324 ture Certificate Policy and Certification Practices Framework.
1325 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 1326 [CFS⁺03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet
1327 x.509 public key infrastructure certificate policy and certification
1328 practices framework. [http://www.ietf.org/internet-drafts/draft-](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt)
1329 [ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 1330 [DPA00] Data protection act 1998. [http://www.legislation.hmso.gov.uk/-](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm)
1331 [acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm), March 2000.
- 1332 [Eur00] EuroPKI Certificate Policy. [http://www.europki.org/ca/root/-](http://www.europki.org/ca/root/cps/en_cp.pdf)
1333 [cps/en_cp.pdf](http://www.europki.org/ca/root/cps/en_cp.pdf), October 2000. Version 1.1.
- 1334 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-
1335 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,
1336 December 1999. Version 1.0.
- 1337 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.
1338 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.
1339 Version 1.1.

- 1340 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.
1341 <http://www.globus.org/security/v2.0/index.html>.
- 1342 [Glob] Globus. Grid security infrastructure for globus toolkit 3.
1343 <http://www.globus.org/security/GSI3/index.html>.
- 1344 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 1345 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String
1346 Representation of Standard Attribute Syntaxes. <http://www.rfc-editor.org/rfc/rfc1778.txt>, March 1995.
1347
- 1348 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public
1349 key infrastructure certificate and certificate revocation list (crl)
1350 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 1351 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 1352 [Moc87] P. Mockapetris. Domain names - concepts and facilities.
1353 <http://www.rfc-editor.org/rfc/rfc1034.txt>, November 1987.
- 1354 [NCS99] National Computational Science Alliance Certificate Pol-
1355 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html)
1356 [Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html), June 1999.
- 1357 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-](http://www.digsigtrust.com/-certificates/policy/tsindex.html)
1358 [certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 1359 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight
1360 Directory Access Protocol (v3): Attribute Syntax Definitions.
1361 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.