

UK e-Science Certification Authority  
Certificate Policy and Certification Practices  
Statement  
ChangeLog Version 1.3-1.4-2

Jens G Jensen

~~CCLRC~~Science and Technology Facilities Council

Rutherford Appleton Laboratory

26 Nov 2007



# Contents

- 1 INTRODUCTION 11**
  - 1.1 Overview . . . . . 11
    - 1.1.1 General definitions . . . . . 11
  - 1.2 Identification . . . . . 16
  - 1.3 Community and Applicability . . . . . 16
    - 1.3.1 Certification authorities . . . . . 16
    - 1.3.2 Registration authorities . . . . . 17
    - 1.3.3 End entities (Subscribers) . . . . . 17
    - 1.3.4 Applicability . . . . . 17
  - 1.4 Contact Details . . . . . 17
    - 1.4.1 Specification administration organisation . . . . . 17
    - 1.4.2 Contact person . . . . . 18
    - 1.4.3 Person determining CPS suitability for the policy . . . 18
  
- 2 GENERAL PROVISIONS 19**
  - 2.1 Obligations . . . . . 19
    - 2.1.1 CA obligations . . . . . 19
    - 2.1.2 RA obligations . . . . . 20
    - 2.1.3 Subscriber obligations . . . . . 21
    - 2.1.4 Relying party obligations . . . . . 23
    - 2.1.5 Repository obligations . . . . . 23
  - 2.2 Liability . . . . . 24
    - 2.2.1 CA liability . . . . . 24
    - 2.2.2 RA liability . . . . . 24
  - 2.3 Financial Responsibility . . . . . 24

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

2.8.7 Other information release circumstances . . . . . 30  
2.9 Intellectual Property Rights . . . . . 30

**3 IDENTIFICATION AND AUTHENTICATION 33**

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

**4 OPERATIONAL REQUIREMENTS 41**

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

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

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

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

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



# Chapter 1

## INTRODUCTION

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

### 1.1 Overview

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

This document was issued on 26 Nov 2007. A second update was issued 03 Dec 2007, fixing a typo.

THIS DOCUMENT IS THE CHANGELOG VERSION BETWEEN VERSIONS 1.3 AND 1.4. 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	<p>The process of establishing that individuals, organisations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. This process corresponds to the second process involved with identification, as shown in the definition of “identification” below. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organisation, or device. Thus, it is said that a digital signature of a message authenticates the message’s sender.</p>
Certificate Policy (CP)	<p>A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions.</p>
Certificate Revocation List (CRL)	<p>A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.</p>
Certification Authority (CA)	<p>An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole lifetime.</p>

Certification Practices Statement (CPS)	A statement of the practices, which a certification authority employs in issuing certificates.
CCLRC	Council for the Central Laboratory of the Research Councils. CCLRC is an independent, non-departmental public body of the Office of Science and Technology, part of the Department of Trade and Industry (UK).
GSI	Grid Security Infrastructure. In this document, GSI refers to the Globus GSI as defined in [Gloa] or [Glob].
GridPP Collaboration	UK Particle Physics collaboration funded by PPARC.
Identification	The process of establishing the identity of an individual or organisation, i.e., to show that an individual or organisation is a specific individual or organisation. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organisation corresponds to a real-world identity of an individual or organisation, and (2) establishing that an individual or organisation applying for or seeking access to something under that name is, in fact, the named individual or organisation. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, the issuing CA is the CA that issued the certificate.
NGS	The UK National Grid Service
Personal Information	For the purpose of this document, Personal Information refers to data which is sufficient for the Identification of a Subscriber according to section 3.1.9. Personal Information will always contain a photo of the individual sufficient for Validation of the Subscriber, and the Subscriber's name sufficient to establish reasonable link to the CN according to section 3.1.2.
Policy Qualifier	Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS.
Registration Authority (RA)	An individual or group of people appointed by an organisation that is responsible for Identification and Authentication of certificate subscribers, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Repository	A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.

Robot	A Robot is defined as an independent personal credential, issued to a specific user, which can perform automated client tasks on behalf of the user. Since the private key cannot be passphrase protected (except by exposing the passphrase) and the certificate is not tied to a network identity, the private key must have special protection.
Service	A service a GSI service (see GSI); it is approximately the same as URL <i>scheme</i> (cf. RFC1738), but is usually meaningful only to Globus protocols.
Signed Email	In this document, “Signed Email” means an email that satisfies all of the following: (1) it is <i>not encrypted</i> , (2) it has a valid signature, and (3) the certificate corresponding to the private key that generated the signature is a valid UK e-Science CA certificate, and (4) the sender address is the same as the one in the subject alternative name.
SSL	Secure Sockets Layer. In this document, “SSL” refers to the SSL protocol version 2 or 3, or TLS version 1.0 (RFC2246).
Strong Pass-phrase	In this document, “Strong Pass-phrase” refers to a pass phrase protecting a private key and satisfying the following: it is at least 16 characters long, and contains upper and lower case letters. It is recommended that the pass-phrase contains some non-letter characters in the US-ASCII range (0x20-0x7e) and no letters outside this range.
Subscriber	A person to whom a digital certificate is issued.

Validation	The process of identification of certificate applicants. “Validation” is a subset of “Identification” and refers to identification in the context of establishing the identity of certificate applicants.
------------	---

## 17 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	ChangeLog 1.3-1.4-1
Document date	26 Nov 2007
Effective from	26 Nov 2007

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

21 See also revision history in Appendix A.

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

## 25 1.3 Community and Applicability

### 26 1.3.1 Certification authorities

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

### 29 **1.3.2 Registration authorities**

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

### 37 **1.3.3 End entities (Subscribers)**

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

### 41 **1.3.4 Applicability**

42 Certificates issued are suitable for the following applications:

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

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

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

## 52 **1.4 Contact Details**

### 53 **1.4.1 Specification administration organisation**

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

### 55 **1.4.2 Contact person**

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

58 Dr Jens G Jensen

59 Rutherford Appleton Laboratory

60 \old{Chilton} \new{Harwell Science and Innovation Campus}

61 Didcot

62 Oxon

63 OX11 0QX

64 UK

65

66 Phone: +44 1 235 446104

67 Fax: +44 1 235 445945

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

### 69 **1.4.3 Person determining CPS suitability for the pol-** 70 **icy**

71 The person mentioned in 1.4.2.

## 72 Chapter 2

# 73 GENERAL PROVISIONS

## 74 2.1 Obligations

### 75 2.1.1 CA obligations

76 The CA must:

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

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

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

## 97     **2.1.2 RA obligations**

98     The RA Manager must:

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

114     The RA Operator must:

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

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

### 146 **2.1.3 Subscriber obligations**

147 Subscribers must:

- 148 ● adhere to the procedures published in this document;
- 149 ● generate a key pair using a trustworthy method;

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

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

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

#### 184 **2.1.4 Relying party obligations**

185 A Relying Party should accept the Subscriber's certificate for authentication  
186 purposes if:

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

195 The Relying Party must:

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

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

#### 205 **2.1.5 Repository obligations**

206 The e-Science CA will publish on its web server [CAW] 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.

235 **2.3.3 Administrative processes**

236 No stipulation.

237 **2.4 Interpretation and Enforcement**

238 **2.4.1 Governing law**

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

243 **2.4.2 Severability, survival, merger, notice**

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

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

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

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

261 **2.4.3 Dispute resolution procedures**

262 No stipulation.

## 263 **2.5 Fees**

### 264 **2.5.1 Certificate issuance or renewal fees**

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

### 267 **2.5.2 Certificate access fees**

268 No stipulation.

### 269 **2.5.3 Revocation or status information access fees**

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

### 272 **2.5.4 Fees for other services such as policy information**

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

### 276 **2.5.5 Refund policy**

277 No stipulation.

## 278 **2.6 Publication and Repositories**

### 279 **2.6.1 Publication of CA information**

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

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

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

### 288 **2.6.2 Frequency of publication**

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

### 291 **2.6.3 Access controls**

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

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

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

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

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

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

### 307 **2.6.4 Repositories**

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

## 309 **2.7 Compliance Audit**

### 310 **2.7.1 Frequency of entity compliance audit**

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

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

### 316 **2.7.2 Identity/qualifications of auditor**

317 No stipulation.

### 318 **2.7.3 Auditor's relationship to audited party**

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

### 324 **2.7.4 Topics covered by audit**

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

### 327 **2.7.5 Actions taken as a result of deficiency**

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

### 330 **2.7.6 Communication of results**

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

## 333 **2.8 Confidentiality**

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

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

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

### 346 **2.8.1 Types of information to be kept confidential**

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

### 349 **2.8.2 Types of information not considered confidential**

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

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

### 355 **2.8.3 Disclosure of certificate revocation/suspension in-** 356 **formation**

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

### 359 **2.8.4 Release to law enforcement officials**

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

362 officials who exhibit regular warrant.

### 363 **2.8.5 Release as part of civil discovery**

364 No stipulation.

### 365 **2.8.6 Disclosure upon owner's request**

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

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

### 375 **2.8.7 Other information release circumstances**

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

## 378 **2.9 Intellectual Property Rights**

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

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

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

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

<sup>391</sup> This document typeset with L<sup>A</sup>T<sub>E</sub>X.



## 392 Chapter 3

# 393 IDENTIFICATION AND 394 AUTHENTICATION

### 395 3.1 Initial Registration

#### 396 3.1.1 Types of names

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

400 The name has one of the following forms:

Person	Name of the Subscriber. The name must include at least one given name in full and the full surname. Rôles are not accepted.
Server	Server fully qualified domain name. The name must be in lower case. IP addresses are not accepted.
Service	As server except the name is prefixed with a service name as defined in 7.1.5.

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

401

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

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

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

405       ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

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

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

416       '0' - '9', 'a' - 'z', 'A' - 'Z', '-', '.'

417 that is, digits, US ASCII letters, hyphen, and dot. In addition, names must  
418 be structured according to RFC1034 [Moc87]. For service certificates, the  
419 character '/' is also allowed in the Common Name.420 Email address in server and service certificates must be structured ac-  
421 cording to RFC822 and must be in the "addr-spec" format as defined in  
422 RFC822. The maximal length of an email address is 128 characters. Email  
423 addresses must be encoded as `IA5String` in the name but must not contain  
424 control characters or delete. For personal certificates, email addresses in sub-  
425 ject alternative name must be included as `rfc822Name` and satisfy the same  
426 constraints.

427 See also 7.1.4.

### 3.1.2 Need for names to be meaningful

#### Personal and Robot certificates

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

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

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

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

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

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

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

#### Host and Service certificates

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

### 461 **3.1.3 Rules for interpreting various name forms**

462 No stipulation.

### 463 **3.1.4 Uniqueness of names**

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

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

### 479 **3.1.5 Name claim dispute resolution procedure**

480 No stipulation.

### 481 **3.1.6 Recognition, authentication and role of trade-** 482 **marks**

483 No stipulation.

### 484 **3.1.7 Method to prove possession of private key**

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

### 487 3.1.8 Authentication of organisation identity

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

491 There is no verification of individuals' organisation identity.

### 492 3.1.9 Authentication of individual identity

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

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

Person	The Subscriber goes to the selected RA Operator bringing acceptable Personal Information. The RA will take a photo copy of this data, and keep it for auditing purposes (see section B.1).
Host	The requestor must <i>either</i> go to the RA Operator in person and prove his/her identity as for personal certificates, and confirm that (s)he is responsible for the resources mentioned in the request, <i>or</i> send Signed Email to the RA Operator confirming the request and confirming that the requestor is responsible for the resources in question.
Service	As server certificates (the person responsible for a host is regarded as the person responsible for all services running on that host).
Robot	The Subscriber must prove that the private key is adequately protected (section 2.1.3), and that the robot DN contains the Subscriber's personal DN (section 3.1.2).

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

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

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

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

## 510 **3.2 Routine Re-key**

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

## 513 **3.3 Re-key After Revocation**

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

## 516 **3.4 Revocation Request**

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

521 Authenticated certificate revocation requests may be made by

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

– Mailing the CA manager directly by Signed Email.



## 527 Chapter 4

# 528 OPERATIONAL 529 REQUIREMENTS

### 530 4.1 Certificate Application

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

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

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

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

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

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

## 546 4.2 Certificate Issuance

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

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

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

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

558 If the authentication is unsuccessful, the certificate is not issued and an  
559 e-mail with the reason is sent to the Subscriber or the Subscriber is otherwise  
560 notified by CA or RA staff. In particular, the CA or RA may delete a request  
561 if the Subscriber has made no attempt to authenticate him- or herself within  
562 30 days of submitting the request.

563 All issued certificates are issued under the CP/CPS valid at the time of  
564 issuance.

## 565 4.3 Certificate Acceptance

566 No stipulation.

## 567 4.4 Certificate Suspension and Revocation

### 568 4.4.1 Circumstances for revocation

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

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

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

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

#### 586 4.4.2 Who can request revocation

587 A certificate revocation can be requested by:

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

#### 593 4.4.3 Procedure for revocation request

594 A revocation request is accepted if:

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

599 Any other revocation request is accepted only if the entity requesting the  
600 revocation is properly authenticated.

#### 601 **4.4.4 Revocation request grace period**

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

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

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

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

#### 612 **4.4.5 Circumstances for suspension**

613 The CA does not offer suspension services.

#### 614 **4.4.6 Who can request suspension**

615 No stipulation.

#### 616 **4.4.7 Procedure for suspension request**

617 No stipulation.

#### 618 **4.4.8 Limits on suspension period**

619 No stipulation.

#### 620 **4.4.9 CRL issuance frequency**

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

#### 623 **4.4.10 CRL checking requirements**

624 No stipulation.

625 **4.4.11 On-line revocation/status checking availability**

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

627 **4.4.12 On-line revocation checking requirements**

628 No stipulation.

629 **4.4.13 Other forms of revocation advertisements avail-**  
630 **able**

631 No stipulation.

632 **4.4.14 Checking requirements for other forms of revo-**  
633 **cation advertisements**

634 No stipulation.

635 **4.4.15 Special requirements re key compromise**

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

640 **4.5 Security Audit Procedures**

641 **4.5.1 Types of event recorded**

642 The following events are recorded:

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

648 **4.5.2 Frequency of processing log**

649 No stipulation.

650 **4.5.3 Retention period for audit log**

651 The minimum retention period is 3 years.

652 **4.5.4 Protection of audit log**

653 No stipulation.

654 **4.5.5 Audit log backup procedures**

655 No stipulation.

656 **4.5.6 Audit collection system (internal vs external)**

657 No stipulation.

658 **4.5.7 Notification to event-causing subject**

659 No stipulation.

660 **4.5.8 Vulnerability assessments**

661 No stipulation.

662 **4.6 Records Archival**

663 **4.6.1 Types of event recorded**

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

- 665 • certification requests;
- 666 • issued certificates;

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

673 Each RA must log the following:

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

#### 679 **4.6.2 Retention period for archive**

680 The minimum retention period is 3 years.

#### 681 **4.6.3 Protection of archive**

682 No stipulation.

#### 683 **4.6.4 Archive backup procedures**

684 No stipulation.

#### 685 **4.6.5 Requirements for time-stamping of records**

686 No stipulation.

#### 687 **4.6.6 Archive collection system (internal or external)**

688 No stipulation.

689 **4.6.7 Procedures to obtain and verify archive informa-**  
690 **tion**

691 No stipulation.

692 **4.7 Key Changeover**

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

698 **4.8 Compromise and Disaster Recovery**

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

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

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

707 **4.8.1 Computing resources, software, and/or data are**  
708 **corrupted**

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

710 **4.8.2 Entity public key is revoked**

711 No stipulation.

712 **4.8.3 Entity key is compromised**

713 No stipulation.

714 **4.8.4 Secure facility after a natural or other type of**  
715 **disaster**

716 No stipulation.

717 **4.9 CA Termination**

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

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

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

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



## 733 Chapter 5

# 734 PHYSICAL, PROCEDURAL, 735 AND PERSONNEL 736 SECURITY CONTROLS

### 737 5.1 Physical Controls

#### 738 5.1.1 Site location and construction

739 No stipulation.

#### 740 5.1.2 Physical access

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

#### 745 5.1.3 Power and air conditioning

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

749 **5.1.4 Water exposures**

750 No stipulation.

751 **5.1.5 Fire prevention and protection**

752 No stipulation.

753 **5.1.6 Media storage**

754 No stipulation.

755 **5.1.7 Waste disposal**

756 No stipulation.

757 **5.1.8 Off-site backup**

758 No stipulation.

759 **5.2 Procedural Controls**

760 **5.2.1 Trusted roles**

761 No stipulation.

762 **5.2.2 Number of persons required per task**

763 No stipulation.

764 **5.2.3 Identification and authentication for each role**

765 No stipulation.

## 5.3 Personnel Controls

### 5.3.1 Background, qualifications, experience, and clearance requirements

- The CA Manager must be a paid employee of CCLRC and shall be appointed in writing by the CCLRC Director of e-Science who may at his/her discretion revoke the appointment with no prior notice given.
- The CA Operators must be paid employees of CCLRC and will be appointed by the CA Manager.
- The RA Manager must be a paid employee of the Physical Organisation hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that physical organisation. The RA Manager must be a member of that Department. The OU field of the RA Operator's certificate identifies the Physical Organisation. Normally, the L field identifies the Department where the Manager is appointed, but the L can also be used further to subdivide the RA in the case of very large or physically distributed RAs managed by a single manager. The Authority will make a declaration to the CA Manager in writing on the organisation's headed note paper. The information that must be contained in this letter is defined by the CA Manager.
- The RA Operator must be a paid employee of the site hosting that Registration Authority and will be appointed by the RA Manager concerned. The RA Manager will make a declaration to the CA Manager in writing on the organisation's headed note paper. If the RA Operator is appointed in a different department from the RA Manager then the letter must be countersigned by an authority for the department in which the Operator is appointed. The information that must be contained in this letter is defined by the CA Manager. RA Operators must have certificates and must adhere also to the Subscribers' Obligations.
- An RA Manager may appoint himself/herself as an RA Operator.
- An RA Manager may appoint any number of RA Operators.

### 5.3.2 Background check procedures

No stipulation.

798 **5.3.3 Training requirements**

799 No stipulation.

800 **5.3.4 Retraining frequency and requirements**

801 No stipulation.

802 **5.3.5 Job rotation frequency and sequence**

803 No stipulation.

804 **5.3.6 Sanctions for unauthorized actions**

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

808 **5.3.7 Contracting personnel requirements**

809 No stipulation.

810 **5.3.8 Documentation supplied to personnel**

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

## 817 Chapter 6

# 818 TECHNICAL SECURITY 819 CONTROLS

## 820 6.1 Key Pair Generation and Installation

### 821 6.1.1 Key pair generation

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

### 824 6.1.2 Private key delivery to entity

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

### 827 6.1.3 Public key delivery to certificate issuer

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

### 830 6.1.4 CA public key delivery to subscribers

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

### 833 **6.1.5 Key sizes**

834 Keys of length less than 1024 bits are not accepted. The CA key is of length  
835 2048 bits.

### 836 **6.1.6 Public key parameters generation**

837 No stipulation.

### 838 **6.1.7 Parameter quality checking**

839 No stipulation.

### 840 **6.1.8 Hardware/software key generation**

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

### 843 **6.1.9 Key usage purposes (as per X.509 v3 key usage 844 field)**

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

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

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

## 850 **6.2 Private Key Protection**

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

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

854

855

The protections above are to be interpreted as follows:

856

- **File system, user only:**

857

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

858

859

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

860

861

862

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

863

864

865

866

- **File system, root only:**

867

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

868

869

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

870

871

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

872

873

874

875

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

876

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

877

878

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

- 885       • **Key token:**

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

### 888 **6.2.1 Standards for cryptographic module**

889 The CA's private key is protected by an HSM certified to FIPS 140-2 Level  
890 3.

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

### 894 **6.2.2 Private key (n out of m) multi-person control**

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

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

### 899 **6.2.3 Private key escrow**

900 Private keys must not be escrowed.

### 901 **6.2.4 Private key backup**

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

### 906 **6.2.5 Private key archival**

907 No stipulation.

### 908 **6.2.6 Private key entry into cryptographic module**

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

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

### 913 **6.2.7 Method of activating private key**

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

### 917 **6.2.8 Method of deactivating private key**

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

### 921 **6.2.9 Method of destroying private key**

922 No stipulation.

## 923 **6.3 Other Aspects of Key Pair Management**

### 924 **6.3.1 Public key archival**

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

### 927 **6.3.2 Usage periods for the public and private keys**

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

## 930 **6.4 Activation Data**

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

### 935 **6.4.1 Activation data generation and installation**

936 No stipulation.

### 937 **6.4.2 Activation data protection**

938 See section 6.4.

### 939 **6.4.3 Other aspects of activation data**

940 No stipulation.

## 941 **6.5 Computer Security Controls**

### 942 **6.5.1 Specific computer security technical requirements**

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

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

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

953 **6.5.2 Computer security rating**

954 No stipulation.

955 **6.6 Life-Cycle Technical Controls**

956 **6.6.1 System development controls**

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

959 **6.6.2 Security management controls**

960 No stipulation.

961 **6.6.3 Life cycle security ratings**

962 No stipulation.

963 **6.7 Network Security Controls**

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

967 **6.8 Cryptographic Module Engineering Con-**  
968 **trols**

969 No stipulation.



## 970 Chapter 7

# 971 CERTIFICATE AND CRL 972 PROFILES

### 973 7.1 Certificate Profile

#### 974 7.1.1 Version number

975 X.509.v3

#### 976 7.1.2 Certificate extensions

977 Host and service certificates have the same extensions.

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

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

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

987 **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
Subject Alternative Name (personal/robot)	Subject's personal email address
Subject Alternative Name (server/service)	Server's Fully Qualified Domain Name
Issuer Alternative Name	CA email
CRL Distribution Points	HTTP URL of CRL
Netscape Cert Type	Personal, Robot: SSL Client, S/MIME  Personal: (optionally) object signing  Server, service: SSL Client, SSL Server
Netscape Comment	"UK e-Science XXX Certificate" where "XXX" is "User", "Host", "Service", or "Robot".
Netscape CA Revocation URL	HTTP URL of CRL
Netscape Revocation URL	HTTP URL of CRL

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

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

990 **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
Signature Algorithm	sha1WithRSAEncryption

991 **7.1.3 Algorithm object identifiers**

992 No stipulation.

993 **7.1.4 Name forms**

994 **CA certificate**

995 Issuer:

996 /C=UK/O=eScienceRoot/OU=Authority/L=Root/CN=CA  
 997 /C=UK/O=eScienceRoot/OU=Authority/CN=UK e-Science Root

998 Subject:

999 /C=UK/O=eScienceCA/OU=Authority/CN=CA  
 1000 /C=UK/O=eScienceCA/OU=Authority/CN=UK e-Science CA

1001 Note that the subject has /C=UK/O=eScienceCA/\* to avoid having the  
 1002 root sign in the same namespace as the CA described in this CP/CPS.

1003 **End Entity Certificate**

1004 Issuer: is the CA's subject DN.

1005 Subject: The subject field contains the Distinguished Name of the entity  
1006 with the following attributes:

Country Name	UK
Organisation Name	eScience
Organizational Unit	Name of physical organisation hosting the RA approving the Subject's request
Locality	Location within the organisation where the RA is appointed.
CommonName	Personal and robot: Name and surname of Subscriber;  Host: FQDN of host;  Service: FQDN of host prefixed by the service name (see 7.1.5) and a '/' (e.g. CN=ldap/ldap.rl.ac.uk).
CommonName	Robots have an additional CN of the form <b>Robot: type</b> .
SubjectAltName	FQDN of server

1007 Important notes:

- 1008 • The DN of EEs is preserved across the CA certificate rollover.
- 1009 • The CN in a personal certificate may contain additional text string,  
1010 as described in section 3.1.2. Likewise, the additional robot CN may  
1011 contain an additional text string, as described in the same section.

1012 The name of the special CA operator (see section 3.1.2) certificate is

1013 `/C=UK/O=eScience/OU=Authority/L=CLRC/CN=ca-operator`

1014 The email address in host and service certificates must be that of one  
1015 or more people responsible for the server in question, and need not be a  
1016 personal address. Host certificates should not have “host” as a service, i.e.  
1017 they should have `CN=host.univ.ac.uk` and not `CN=host/host.univ.ac.uk`  
1018 if they are used with non-Globus servers.

1019 The CA will issue certificates for a given service if and only if:

- 1020 • the service has been defined by IANA [IAN]; or
- 1021 • The CA Manager has approved the service.

1022 It is the responsibility of the CA Manager to define the non-IANA services  
1023 allowed by the CA. For each service, the CA Manager must provide

- 1024 • the name of the service,
- 1025 • the default port number,
- 1026 • a short description of the service,
- 1027 • a reference URI.

1028 The CA Manager must ensure that services are unique in name.

1029 It is the responsibility of the CA Manager to define the robot types sup-  
1030 ported by the CA. For each robot type, the CA Manager must provide

- 1031 • the name of the robot type (as in `CN=Robot: type`);
- 1032 • The exact profile of the robot (extensions);
- 1033 • Purposes for which the robot certificate is to be used;
- 1034 • Purposes for which using the robot certificate is explicitly forbidden, if  
1035 any;
- 1036 • Additional qualifications a requestor must have and prove to an RA in  
1037 order to successfully obtain a robot certificate, if any.

### 1038 7.1.5 Name constraints

1039 No stipulation<sup>1</sup>.

---

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

### 1040 **7.1.6 Certificate policy Object Identifier**

1041 Certificates contain in the PolicyInformation extension the policyIdentifier  
1042 containing the OID of the CP/CPS under which they were issued. Addition-  
1043 ally, robot certificates contain an 1SCP robot OID.

### 1044 **7.1.7 Usage of Policy Constraints extensions**

1045 No stipulation.

### 1046 **7.1.8 Policy qualifier syntax and semantics**

1047 No stipulation.

### 1048 **7.1.9 Processing semantics for the critical certificate** 1049 **policy**

1050 No stipulation.

## 1051 **7.2 CRL Profile**

### 1052 **7.2.1 Version number**

1053 X.509.v1: Version 1 is required for compatibility with Netscape Communi-  
1054 cator.

### 1055 **7.2.2 CRL and CRL Entry Extensions**

1056 No stipulation.

# 1057 Chapter 8

## 1058 SPECIFICATION 1059 ADMINISTRATION

### 1060 8.1 Specification Change Procedures

1061 We distinguish between different types of modifications to the CP/CPS:

1062 *Editorial updates:* editorial changes to the CPS, including replacing fields  
1063 with “No stipulation”, as long as they do not affect procedure or compromise  
1064 security. These changes are announced on the CA web site but no advance  
1065 warning will be given.

1066 *Procedure updates:* minor changes to the CPS that do not compromise secu-  
1067 rity in any way. E.g. changes to the verification or issuing procedure that  
1068 do not affect security. Subscribers and relying parties will not be warned of  
1069 such changes in advance but RAs will be given at least one week’s notice of  
1070 changes that affect their procedures.

1071 *Technical updates:* e.g. changes to the extensions in the issued certificates.  
1072 Such changes will be announced on the CA web site and on appropriate  
1073 mailing lists at least 14 days in advance.

1074 *Security updates:* changes that affect the security, e.g. changes to the minimal  
1075 requirements for verifying requests, or changing the key sizes. These changes  
1076 will be announced at least 30 days in advance on the CA web site, and to  
1077 appropriate mailing lists, including the EU Grid PMA mailing list. However,  
1078 urgent security fixes may be carried out without advance warning and then  
1079 documented in the CPS. These will be announced in the same manner.

1080 *Policy updates:* e.g. changes to the namespace, or introducing subordinate  
1081 CAs. A proposal will be announced at least 30 days in advance on the CA

1082 web site and appropriate mailing lists.

1083 *Termination:* A scheduled termination of the CA is announced on the CA  
1084 web site and appropriate mailing lists at least 60 days in advance.

## 1085 **8.2 Publication and Notification Policies**

1086 This CP/CPS is available at [CAW]. All changes are announced on the CA  
1087 web site and a changelog is available. In addition, changes are announced to  
1088 appropriate mailing lists, depending on the type of change, as described in  
1089 section 8.1.

1090 There is a mailing list for RA Managers and Operators. Only subscribers  
1091 can post to the mailing list. Only subscribers can read the archives.

## 1092 **8.3 CPS Approval Procedures**

1093 No stipulation.



# 1094 Appendix A

## 1095 Revision History

1096

Version	OID	Date	Comments
0.1		4 September 2001	Initial unapproved release
0.3		30 January 2002	Andrew's changes
0.4		13 March 2002	Jens' changes
0.5		April/May 2002	Tim's changes
0.6		28 May 2002	draft version
0.7	1.1	17 July 2002	final draft
0.8	1.2	10 October 2002	Removed identification by telephone, made specification of host verification more precise, added missing RFC2527 entries.
0.9	1.3	31 March 2003	Update to request extensions. Describe renewal. Tightened
1.0	1.4	30 October 2003	up several parts, including Applicability, personal information stored, etc.
1.1	1.5	04 March 2005	Documented that we use SHA1 to sign.
1.2	1.6	15 May 2005	Documented CA upgrade, Data protection act, and some codifications of existing practice.
1.3	1.7	4 August 2006	CA rollover, signing key online, robots.
<u>1.4</u>	<u>1.8</u>	<u>26 Nov 2007</u>	Security rollover, plus minor security-related updates (only). 2nd update fixed year.

1097

<sup>1098</sup> The OID in the table is the final two digits of the actual OID, as defined in  
<sup>1099</sup> section 1.2.



# 1100 Appendix B

## 1101 Compliance with Laws and 1102 Regulations

1103 The UK e-Science CA operates under English Law. See section 2.4.1.

1104 In the case an RA Operator or CA Operator cannot complete his or her  
1105 operations without violating rules set forth in this Appendix, the Operator  
1106 must not complete the operation and must notify the CA Manager, and, if  
1107 applicable, his or her RA Manager.

### 1108 B.1 The Data Protection Act

1109 The Data Protection Act 1998 (DPA) [DPA00].

#### 1110 B.1.1 Definitions

- 1111 • The *data controller* is the CA Manager, the person mentioned in 1.4.2.
- 1112 • The *data processor* is any RA Manager or Operator.
- 1113 • The *data subject* is a Subscriber requesting a certificate, or an RA  
1114 Operator or a CA Operator being appointed as such by the CA.
- 1115 • *Data* is to be understood as defined in DPA section I.1.
- 1116 • *Processing Data* is to be understood as defined in DPA section I.1.
- 1117 • Throughout this Appendix, *Personal Data* means Data which is Per-  
1118 sonal Data as defined in DPA section I.1 but which is not *Sensitive*  
1119 *Personal Data* as defined in DPA section I.2.

- 1120 • *Personal Information* is defined in section 1.1.1 of this document. For  
1121 the purposes of the DPA,
- 1122     – the photo id is considered Sensitive Personal Data;
- 1123     – all other parts of Personal Information are considered Personal  
1124 Data.

### 1125 B.1.2 Preliminaries

1126 The *intent* of Processing Data by the UK e-Science CA is that minimal and  
1127 adequate Personal Information is stored and Processed in order that the UK  
1128 e-Science CA may operate according to the policy and practices described  
1129 in this CP/CPS, including being an internationally approved medium level  
1130 CA.

### 1131 B.1.3 Data

1132 The UK e-Science CA stores the following Data:

- 1133 1. The CA publishes on its web page, and may publish by other methods,  
1134 the Subscriber's *certificate* and thus all information contained therein,  
1135 including the Subscriber's name;
- 1136 2. The CA logs and stores all Subscriber and RA interactions with the  
1137 CA's online service, in order to satisfy the requirements of sections 4.5  
1138 and 4.6 of this CP/CPS;
- 1139 3. The RA Operator Processes Personal Information, and possibly other  
1140 Data, as described in section B.1.5;
- 1141 4. The CA stores authorisation information about the RA Manager and  
1142 Operators sufficient to convince the CA that the RA Manager and  
1143 Operators satisfy the conditions of section 5.3.1 and that the CA has the  
1144 RA Manager's assurance that the RA Operator will operate according  
1145 to this CP/CPS;
- 1146 5. For host and service certificates, it may be necessary to obtain and store  
1147 Personal Data that proves to the RA Operator's satisfaction that Sub-  
1148 scriber is responsible system administrator for the resource for which  
1149 the Subscriber requests a certificate, in accordance with sections 2.1.2,  
1150 2.1.3, and 3.1.9;

- 1151 6. It may be necessary to obtain and store Personal Data to prove to the  
1152 RA Operator's satisfaction that the Subscriber is entitled to a certifi-  
1153 cate from the UK e-Science CA, cf. section 1.3.3.

1154 Notwithstanding the above, the Data Processed by the UK e-Science CA is  
1155 subject to the following restrictions:

- 1156 • The UK e-Science CA must not Process or attempt to Process any  
1157 Sensitive Personal Data *except* the photo id.
- 1158 • Personal Data and Sensitive Personal Data must be relevant and ade-  
1159 quate for the purpose for which it is Processed.
- 1160 • The UK e-Science CA must Process Personal Information only as de-  
1161 fined in this Appendix, and in accordance with the DPA.

#### 1162 B.1.4 Consent

1163 By submitting Data to the online CA ([CAW]), the Subscriber is considered  
1164 to have given consent that the submitted Data may be Processed by the  
1165 e-Science CA (there is a notice to this effect on the web page). By present-  
1166 ing Personal Information to the RA Operator, the Subscriber is deemed to  
1167 have given consent that this information may be Processed according to the  
1168 purposes described in this document, and stored according to the procedures  
1169 described in this document (there is a notice to this effect on the web page).  
1170 By applying for RA Operator or CA Operator status, the RA Operator or CA  
1171 Operator is deemed to have consented that the CA can Process the Data as  
1172 described below (there is a notice to this effect in the template appointment  
1173 letters provided by the CA).

#### 1174 B.1.5 Processing

1175 The CA permits that Personal Information is Processed as follows:

- 1176 1. The CA Operator or RA Operator obtains Personal Information or  
1177 other Data from the Subscriber or from another Operator relevant and  
1178 adequate for the purposes described below;
- 1179 2. A photocopy of the Personal Information is made for the purposes  
1180 described below;

- 1181 3. The photocopy of Personal Information is subsequently accessed only  
1182 for the purposes described below;
- 1183 4. Subscriber's email address is obtained and used only for the purposes  
1184 described below;
- 1185 5. Relevant and adequate information is Processed to satisfy section 4.5  
1186 of this CP/CPS in accordance with sections 4.5 and 4.6.

### 1187 **B.1.6 Purpose**

1188 The UK e-Science CA Processes Personal Information for the following pur-  
1189 poses:

- 1190 1. Identification of a Subscriber;
- 1191 2. Subsequent auditing of the Identification process, for the case where the  
1192 UK e-Science CA must prove the link from the DN to the Subscriber's  
1193 real identity;
- 1194 3. Release of Personal Information under the circumstances described in  
1195 section 2.8 and according to the procedures described in the same sec-  
1196 tion;
- 1197 4. To maintain the uniqueness of the DN to the extent described in sec-  
1198 tion 3.1.4;
- 1199 5. For RA and CA Operators, to check to the CA Manager's satisfaction  
1200 that the RA or CA Operator is duly authorised by appointment letter  
1201 to operate according to this CP/CPS and that the RA Manager and  
1202 Operator satisfy the conditions described in section 5.3.1;
- 1203 6. Adequate Personal Information is Processed to satisfy the auditing re-  
1204 quirements set forth in sections 2.7, 4.5 and 4.6 of this CP/CPS;
- 1205 7. Email address is used only to notify the Subscriber that:
- 1206 • A new certificate has been issued to the Subscriber;
  - 1207 • A certificate held by the Subscriber is about to expire.

1208 Data may be used for statistical purposes

- 1209 • only with the Data Controller's permission; and

- 1210     • if there is reasonable cause; and
- 1211     • if the published information contain neither Personal Data nor Sensitive  
1212       Personal Data, and no Personal Data or Sensitive Personal Data can  
1213       be derived from it; and
- 1214     • the Processing associated with and required for statistical purposes are  
1215       done in accordance with the DPA section 33.

1216 Any other use of Personal Information is explicitly forbidden.

### 1217 **B.1.7 Data Release**

1218 Circumstances requiring Processing of Personal Information include, but are  
1219 not necessarily limited to, the following cases:

- 1220     1. A CA Manager or Operator is considered to have breached CA Obli-  
1221       gations (section 2.1.1);
- 1222     2. An RA Manager or Operator is considered to have breached RA Obli-  
1223       gations (section 2.1.2);
- 1224     3. A Subscriber is considered to have breached Subscriber's Obligations  
1225       (section 2.1.3);
- 1226     4. Release of information as described in section 2.8, including any release  
1227       required by UK law;
- 1228     5. Release of information as required for auditing purposes, including com-  
1229       pliance audit as described in section 2.7.

1230 In each case, the UK e-Science CA shall ensure that only the adequate and  
1231 relevant information is released and that the information is Processed law-  
1232 fully and in accordance with the rules of sections B.1.5 and B.1.6, and in  
1233 accordance with the DPA.

### 1234 **B.1.8 Data Maintenance**

1235 There is no requirement for keeping Personal Information Processed by the  
1236 RA up to date, except to the extent required to satisfy the RA Operator  
1237 that the information mentioned in 5 and 6 in section B.1.3 is still valid if and  
1238 when certificates that required this information prior to their approval are  
1239 being renewed.

1240 It is the RA Manager's responsibility to ensure that the Data Processed  
1241 by the CA concerning his or her RA or any Manager or Operator associated  
1242 with that RA is kept up to date, and inform the CA of any update.

### 1243 **B.1.9 Data Retention**

1244 Personal Information shall be kept by the UK e-Science CA for as long as is  
1245 necessary:

- 1246 1. Personal Information used to obtain a personal certificate with a certain  
1247 DN shall be kept for as long as the Subscriber has a valid certificate  
1248 with this DN, including renewals of the certificate, and for a period  
1249 beyond the expiry or revocation of the latest certificate held by the  
1250 Subscriber necessary to satisfy the retention requirements described in  
1251 section 4.6;
- 1252 2. Data used to obtain a host or service certificate shall be kept for as  
1253 long as the Subscriber is responsible administrator for the resource for  
1254 which the certificate was obtained, and for a period beyond the expiry  
1255 or revocation of the latest certificate held by the Subscriber, or beyond  
1256 the administrator rights being passed on to someone else, necessary to  
1257 satisfy the retention requirements described in section 4.6.
- 1258 3. Data used by the CA Manager to authorise RA Managers and Op-  
1259 erators must be kept for a period beyond the termination of the RA  
1260 necessary to satisfy the requirements described in section 4.6. For the  
1261 termination of the CA, the conditions in sections 4.6.2 and 4.9 apply.

1262 It is the responsibility of the RA Manager to ensure that appropriate techni-  
1263 cal and organisational measures are taken against unlawful or unauthorised  
1264 Processing of Data held by the RA. It is the responsibility of the CA Manager  
1265 to ensure that appropriate technical and organisational measures are taken  
1266 against unlawful or unauthorised Processing of Data held by the CA.

### 1267 **B.1.10 Data Termination**

1268 It is the responsibility of the RA Manager to ensure that Personal Information  
1269 held and Processed by the RA is adequately destroyed by the end of the  
1270 retention period. It is the responsibility of the CA Manager to ensure that  
1271 Personal Information held and Processed by the CA is adequately destroyed  
1272 by the end of the retention period.

# Bibliography

- 1274 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate  
1275 policy model. [http://www.gridforum.org/2\\_SEC/pdf/Draft-](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf)  
1276 [GGF-CP-06.pdf](http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf), September 2001.
- 1277 [BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform resource  
1278 locators. <http://www.rfc-editor.org/rfc/rfc1738.txt>, December  
1279 1994.
- 1280 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 1281 [Cec01] R. Cecchini. INFN CA CP/CPS. [http://security.fi.infn.it/CA/-](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf)  
1282 [CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 1283 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-  
1284 ture Certificate Policy and Certification Practices Framework.  
1285 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 1286 [CFS<sup>+</sup>03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet  
1287 x.509 public key infrastructure certificate policy and certification  
1288 practices framework. [http://www.ietf.org/internet-drafts/draft-](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt)  
1289 [ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 1290 [DPA00] Data protection act 1998. [http://www.legislation.hmso.gov.uk/-](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm)  
1291 [acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm), March 2000.
- 1292 [Eur00] EuroPKI Certificate Policy. [http://www.europki.org/ca/root/-](http://www.europki.org/ca/root/cps/en_cp.pdf)  
1293 [cps/en\\_cp.pdf](http://www.europki.org/ca/root/cps/en_cp.pdf), October 2000. Version 1.1.
- 1294 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-  
1295 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,  
1296 December 1999. Version 1.0.
- 1297 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.  
1298 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.  
1299 Version 1.1.

- 1300 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.  
1301 <http://www.globus.org/security/v2.0/index.html>.
- 1302 [Glob] Globus. Grid security infrastructure for globus toolkit 3.  
1303 <http://www.globus.org/security/GSI3/index.html>.
- 1304 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 1305 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String  
1306 Representation of Standard Attribute Syntaxes. [http://www.rfc-](http://www.rfc-editor.org/rfc/rfc1778.txt)  
1307 [editor.org/rfc/rfc1778.txt](http://www.rfc-editor.org/rfc/rfc1778.txt), March 1995.
- 1308 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public  
1309 key infrastructure certificate and certificate revocation list (crl)  
1310 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 1311 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 1312 [Moc87] P. Mockapetris. Domain names - concepts and facilities.  
1313 <http://www.rfc-editor.org/rfc/rfc1034.txt>, November 1987.
- 1314 [NCS99] National Computational Science Alliance Certificate Pol-  
1315 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html)  
1316 [Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html), June 1999.
- 1317 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-](http://www.digsigtrust.com/-certificates/policy/tsindex.html)  
1318 [certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 1319 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight  
1320 Directory Access Protocol (v3): Attribute Syntax Definitions.  
1321 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.