



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

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

30 October 2003



# Contents

- 1 INTRODUCTION 11**
  - 1.1 Overview . . . . . 11
    - 1.1.1 General definitions . . . . . 11
  - 1.2 Identification . . . . . 15
  - 1.3 Community and Applicability . . . . . 16
    - 1.3.1 Certification authorities . . . . . 16
    - 1.3.2 Registration authorities . . . . . 16
    - 1.3.3 End entities (Subscribers) . . . . . 16
    - 1.3.4 Applicability . . . . . 16
  - 1.4 Contact Details . . . . . 17
    - 1.4.1 Specification administration organisation . . . . . 17
    - 1.4.2 Contact person . . . . . 17
    - 1.4.3 Person determining CPS suitability for the policy . . . 17
  
- 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 . . . . . 21
    - 2.1.5 Repository obligations . . . . . 22
  - 2.2 Liability . . . . . 22
    - 2.2.1 CA liability . . . . . 22
    - 2.2.2 RA liability . . . . . 22
  - 2.3 Financial Responsibility . . . . . 23

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

2.8.7	Other information release circumstances . . . . .	28
2.9	Intellectual Property Rights . . . . .	28
<b>3</b>	<b>IDENTIFICATION AND AUTHENTICATION</b>	<b>29</b>
3.1	Initial Registration . . . . .	29
3.1.1	Types of names . . . . .	29
3.1.2	Need for names to be meaningful . . . . .	30
3.1.3	Rules for interpreting various name forms . . . . .	30
3.1.4	Uniqueness of names . . . . .	31
3.1.5	Name claim dispute resolution procedure . . . . .	31
3.1.6	Recognition, authentication and role of trademarks . . . . .	31
3.1.7	Method to prove possession of private key . . . . .	31
3.1.8	Authentication of organisation identity . . . . .	31
3.1.9	Authentication of individual identity . . . . .	31
3.2	Routine Re-key . . . . .	32
3.3	Re-key After Revocation . . . . .	33
3.4	Revocation Request . . . . .	33
<b>4</b>	<b>OPERATIONAL REQUIREMENTS</b>	<b>35</b>
4.1	Certificate Application . . . . .	35
4.2	Certificate Issuance . . . . .	35
4.3	Certificate Acceptance . . . . .	36
4.4	Certificate Suspension and Revocation . . . . .	36
4.4.1	Circumstances for revocation . . . . .	36
4.4.2	Who can request revocation . . . . .	36
4.4.3	Procedure for revocation request . . . . .	37
4.4.4	Revocation request grace period . . . . .	37
4.4.5	Circumstances for suspension . . . . .	37
4.4.6	Who can request suspension . . . . .	37
4.4.7	Procedure for suspension request . . . . .	38
4.4.8	Limits on suspension period . . . . .	38
4.4.9	CRL issuance frequency . . . . .	38
4.4.10	CRL checking requirements . . . . .	38
4.4.11	On-line revocation/status checking availability . . . . .	38

4.4.12	On-line revocation checking requirements . . . . .	38
4.4.13	Other forms of revocation advertisements available . . .	38
4.4.14	Checking requirements for other forms of revocation advertisements . . . . .	38
4.4.15	Special requirements re key compromise . . . . .	39
4.5	Security Audit Procedures . . . . .	39
4.5.1	Types of event recorded . . . . .	39
4.5.2	Frequency of processing log . . . . .	39
4.5.3	Retention period for audit log . . . . .	39
4.5.4	Protection of audit log . . . . .	39
4.5.5	Audit log backup procedures . . . . .	39
4.5.6	Audit collection system (internal vs external) . . . . .	40
4.5.7	Notification to event-causing subject . . . . .	40
4.5.8	Vulnerability assessments . . . . .	40
4.6	Records Archival . . . . .	40
4.6.1	Types of event recorded . . . . .	40
4.6.2	Retention period for archive . . . . .	41
4.6.3	Protection of archive . . . . .	41
4.6.4	Archive backup procedures . . . . .	41
4.6.5	Requirements for time-stamping of records . . . . .	41
4.6.6	Archive collection system (internal or external) . . . . .	41
4.6.7	Procedures to obtain and verify archive information . . .	41
4.7	Key Changeover . . . . .	41
4.8	Compromise and Disaster Recovery . . . . .	41
4.8.1	Computing resources, software, and/or data are cor- rupted . . . . .	42
4.8.2	Entity public key is revoked . . . . .	42
4.8.3	Entity key is compromised . . . . .	42
4.8.4	Secure facility after a natural or other type of disaster .	42
4.9	CA Termination . . . . .	42
<b>5</b>	<b>PHYSICAL, PROCEDURAL, AND PERSONNEL SECUR-</b> <b>RITY CONTROLS</b>	<b>45</b>
5.1	Physical Controls . . . . .	45

5.1.1	Site location and construction . . . . .	45
5.1.2	Physical access . . . . .	45
5.1.3	Power and air conditioning . . . . .	45
5.1.4	Water exposures . . . . .	46
5.1.5	Fire prevention and protection . . . . .	46
5.1.6	Media storage . . . . .	46
5.1.7	Waste disposal . . . . .	46
5.1.8	Off-site backup . . . . .	46
5.2	Procedural Controls . . . . .	46
5.2.1	Trusted roles . . . . .	46
5.2.2	Number of persons required per task . . . . .	46
5.2.3	Identification and authentication for each role . . . . .	46
5.3	Personnel Controls . . . . .	47
5.3.1	Background, qualifications, experience, and clearance requirements . . . . .	47
5.3.2	Background check procedures . . . . .	47
5.3.3	Training requirements . . . . .	48
5.3.4	Retraining frequency and requirements . . . . .	48
5.3.5	Job rotation frequency and sequence . . . . .	48
5.3.6	Sanctions for unauthorized actions . . . . .	48
5.3.7	Contracting personnel requirements . . . . .	48
5.3.8	Documentation supplied to personnel . . . . .	48
<b>6</b>	<b>TECHNICAL SECURITY CONTROLS</b>	<b>49</b>
6.1	Key Pair Generation and Installation . . . . .	49
6.1.1	Key pair generation . . . . .	49
6.1.2	Private key delivery to entity . . . . .	49
6.1.3	Public key delivery to certificate issuer . . . . .	49
6.1.4	CA public key delivery to subscribers . . . . .	49
6.1.5	Key sizes . . . . .	50
6.1.6	Public key parameters generation . . . . .	50
6.1.7	Parameter quality checking . . . . .	50
6.1.8	Hardware/software key generation . . . . .	50

6.1.9	Key usage purposes (as per X.509 v3 key usage field)	50
6.2	Private Key Protection	50
6.2.1	Standards for cryptographic module	50
6.2.2	Private key (n out of m) multi-person control	50
6.2.3	Private key escrow	51
6.2.4	Private key backup	51
6.2.5	Private key archival	51
6.2.6	Private key entry into cryptographic module	51
6.2.7	Method of activating private key	51
6.2.8	Method of deactivating private key	51
6.2.9	Method of destroying private key	51
6.3	Other Aspects of Key Pair Management	52
6.3.1	Public key archival	52
6.3.2	Usage periods for the public and private keys	52
6.4	Activation Data	52
6.4.1	Activation data generation and installation	52
6.4.2	Activation data protection	52
6.4.3	Other aspects of activation data	52
6.5	Computer Security Controls	52
6.5.1	Specific computer security technical requirements	52
6.5.2	Computer security rating	53
6.6	Life-Cycle Technical Controls	53
6.6.1	System development controls	53
6.6.2	Security management controls	53
6.6.3	Life cycle security ratings	53
6.7	Network Security Controls	53
6.8	Cryptographic Module Engineering Controls	53
<b>7</b>	<b>CERTIFICATE AND CRL PROFILES</b>	<b>55</b>
7.1	Certificate Profile	55
7.1.1	Version number	55
7.1.2	Certificate extensions	55
7.1.3	Algorithm object identifiers	57

<i>CONTENTS</i>	9
7.1.4 Name forms . . . . .	57
7.1.5 Name constraints . . . . .	58
7.1.6 Certificate policy Object Identifier . . . . .	58
7.1.7 Usage of Policy Constraints extensions . . . . .	58
7.1.8 Policy qualifier syntax and semantics . . . . .	58
7.1.9 Processing semantics for the critical certificate policy .	59
7.2 CRL Profile . . . . .	59
7.2.1 Version number . . . . .	59
7.2.2 CRL and CRL Entry Extensions . . . . .	59
<b>8 SPECIFICATION ADMINISTRATION</b>	<b>61</b>
8.1 Specification Change Procedures . . . . .	61
8.2 Publication and Notification Policies . . . . .	62
8.3 CPS Approval Procedures . . . . .	62
<b>A Revision History</b>	<b>63</b>



# 1 Chapter 1

## 2 INTRODUCTION

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

### 5 1.1 Overview

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

7 This document was issued on 30 October 2003 and took effect on 14  
8 November 2003.

#### 9 1.1.1 General definitions

10 The document makes use of the following terms:

Activation data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share)
-----------------	--

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

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

Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, the issuing CA is the CA that issued the certificate.
Policy Qualifier	Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS.
Registration Authority (RA)	An individual or group of people appointed by an organisation that is responsible for Identification and Authentication of certificate subscribers, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Repository	A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.
Signed Email	In this document, “Signed Email” means an email that satisfies all of the following: (1) it is <i>not encrypted</i> , (2) it has a valid signature, and (3) the certificate corresponding to the private key that generated the signature is a valid e-Science CA certificate, and (4) the Common Name of the certificate bears a reasonable relation to the sender address of the email.
SSL	Secure Sockets Layer. In this document, “SSL” refers to the SSL protocol version 2 or 3, or TLS version 1.0 (RFC2246).

Strong Pass-phrase	In this document, “Strong Pass-phrase” refers to a pass phrase protecting a private key and satisfying the following: it is at least 16 characters long, and contains upper and lower case letters. It is recommended that the pass-phrase contains some non-letter characters in the US-ASCII range (0x20-0x7e) and no letters outside this range.
Subscriber	A person or server to whom a digital certificate is issued.
Validation	The process of identification of certificate applicants. “Validation” is a subset of “Identification” and refers to identification in the context of establishing the identity of certificate applicants.
Virtual Organisation (VO)	An approved programme activity (e.g. pilot project or regional centre).

## 11 1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	1.0
Document date	30 October 2003
Effective from	14 November 2003
Document OID	1.3.6.1.4.1.11439.1.1.1.1.4

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

15 See also revision history in Appendix A.

## 16 **1.3 Community and Applicability**

### 17 **1.3.1 Certification authorities**

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

### 20 **1.3.2 Registration authorities**

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

### 28 **1.3.3 End entities (Subscribers)**

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

### 31 **1.3.4 Applicability**

32 Certificates issued are suitable for the following applications:

- 33 • SSL or GSI client (all certificates);
- 34 • SSL or GSI server (server and service certificates only);
- 35 • GSI service (service certificates only);
- 36 • Generating GSI proxies (all certificates);

37 In addition, it is permissible to use certificates for email signing. Using certifi-  
38 cates for encryption is not explicitly prohibited but the CA does not support  
39 this purpose.

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

## 42 **1.4 Contact Details**

### 43 **1.4.1 Specification administration organisation**

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

### 45 **1.4.2 Contact person**

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

48 Dr Jens G Jensen  
49 Rutherford Appleton Laboratory  
50 Chilton  
51 Didcot  
52 Oxon  
53 OX11 0QX  
54 UK  
55  
56 Phone: +44 1 235 446104  
57 Fax: +44 1 235 445945  
58 Email: ca-manager@grid-support.ac.uk

### 59 **1.4.3 Person determining CPS suitability for the pol- 60 icsy**

61 The person mentioned in 1.4.2.



## 62 Chapter 2

# 63 GENERAL PROVISIONS

## 64 2.1 Obligations

### 65 2.1.1 CA obligations

66 The CA must:

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

## 81 **2.1.2 RA obligations**

82 The RA Manager must:

- 83 • agree the name of the RA (the values of the OU and L in the DN) with  
84 the CA Manager;
- 85 • define the community of Subscribers for which the RA will approve  
86 requests, and any requirements in addition to those imposed by this  
87 CP/CPS;
- 88 • ensure that (s)he is appointed according to the procedures described in  
89 this CP/CPS;
- 90 • appoint one or more RA Operators according to the procedures de-  
91 scribed in this CP/CPS;
- 92 • ensure that the Operator(s) operate according to the procedures pro-  
93 vided by the CA;
- 94 • in particular, ensure that the RA stores all logs and additional Sub-  
95 scription information securely, and is released only according to the con-  
96 ditions described in section 2.8;
- 97 • provide access to the logs when requested by the CA.

98 The RA Operator must:

- 99 • adhere to all Subscriber's Obligations (2.1.3)
- 100 • accept certification requests from entitled entities;
- 101 • verify the identity of the Subscriber and keep a log of how each Sub-  
102 scription was identified;
- 103 • check that additional location-specific requirements (if any) are fulfilled  
104 (an RA may have more stringent requirements for verifying a request  
105 than the minimum requirements set out in this policy document - in  
106 that case, the RA's web page should list these requirements);
- 107 • provide information to the Subscriber on how to properly maintain a  
108 certificate and the corresponding private key;
- 109 • check that the information provided in the certificate request is correct  
110 as described in section 3.1.9;

- 111 • sign Subscriber's request when and only when all conditions for issuing  
112 a certificate to the Subscriber are fulfilled;
- 113 • Request revocation of a Subscriber's certificate when and only when  
114 the RA Operator is aware that (1) the circumstances for revocation  
115 (4.4.1) are fulfilled, and (2) revocation has not already been requested.

### 116 **2.1.3 Subscriber obligations**

117 Subscribers must:

- 118 • read and adhere to the procedures published in this document;
- 119 • generate a key pair using a trustworthy method;
- 120 • use the certificate for the permitted purposes only;
- 121 • authorise the processing and conservation of personal data (as required  
122 under the Data Protection Act 1998 [DPA00]);
- 123 • take every precaution to prevent any loss, disclosure or unauthorised  
124 access to or use of the private key associated with the certificate, in-  
125 cluding:
  - 126 – (personal certificates) selecting a Strong Pass-phrase;
  - 127 – (personal certificates) protecting the pass-phrase from others;
  - 128 – notifying immediately the e-Science CA and any relying parties if  
129 the private key is lost or compromised;
  - 130 – requesting revocation if the Subscriber is no longer entitled to a  
131 certificate, or if information in the certificate becomes wrong or  
132 inaccurate.

### 133 **2.1.4 Relying party obligations**

134 A Relying Party should accept the Subscriber's certificate for authentication  
135 purposes if:

- 136 • the Relying Party is familiar with the CA's CP and the CPS that  
137 generated the certificate before drawing any conclusion on trust of the  
138 Subscriber's certificate; and

- 139     • the reliance is reasonable and in good faith in light of all circumstances  
140         known to the Relying Party at the time of reliance; and
- 141     • the certificate is used for permitted purposes only; and
- 142     • the Relying Party checked the status of the certificate to their own  
143         satisfaction prior to reliance.

### 144   **2.1.5   Repository obligations**

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

## 147   **2.2    Liability**

### 148   **2.2.1   CA liability**

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

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

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

### 164   **2.2.2   RA liability**

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

169 **2.3 Financial Responsibility**

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

171 **2.3.1 Indemnification by relying parties**

172 No stipulation.

173 **2.3.2 Fiduciary relationships**

174 No stipulation.

175 **2.3.3 Administrative processes**

176 No stipulation.

177 **2.4 Interpretation and Enforcement**

178 **2.4.1 Governing law**

179 Interpretation of this policy is according to UK Law.

180 **2.4.2 Severability, survival, merger, notice**

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

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

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

188 **2.4.3 Dispute resolution procedures**

189 No stipulation.

## 190 **2.5 Fees**

### 191 **2.5.1 Certificate issuance or renewal fees**

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

### 194 **2.5.2 Certificate access fees**

195 No fees are charged for certificate access.

### 196 **2.5.3 Revocation or status information access fees**

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

### 199 **2.5.4 Fees for other services such as policy information**

200 No fees are charged for access to CP and CPS or other CA status informa-  
201 tion. The CA reserves the right to charge a fee for the release of personal  
202 information, as described in section 2.8.6.

### 203 **2.5.5 Refund policy**

204 No stipulation.

## 205 **2.6 Publication and Repositories**

### 206 **2.6.1 Publication of CA information**

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

- 208 • The e-Science CA's certificate;
- 209 • Certificates issued;
- 210 • Certificate Revocation Lists;

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

### 214 **2.6.2 Frequency of publication**

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

### 218 **2.6.3 Access controls**

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

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

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

### 229 **2.6.4 Repositories**

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

## 231 **2.7 Compliance Audit**

### 232 **2.7.1 Frequency of entity compliance audit**

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

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

### 238 **2.7.2 Identity/qualifications of auditor**

239 No stipulation.

### 240 **2.7.3 Auditor's relationship to audited party**

241 An external audit can be performed by any UK government department or  
242 UK academic institution.

### 243 **2.7.4 Topics covered by audit**

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

### 246 **2.7.5 Actions taken as a result of deficiency**

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

### 249 **2.7.6 Communication of results**

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

## 252 **2.8 Confidentiality**

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

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

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

### 264 **2.8.1 Types of information to be kept confidential**

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

### 269 **2.8.2 Types of information not considered confidential**

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

273 Statistics regarding certificates issuance and revocation contain no per-  
274 sonal information and is not considered confidential.

### 275 **2.8.3 Disclosure of certificate revocation/suspension in-** 276 **formation**

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

### 279 **2.8.4 Release to law enforcement officials**

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

### 283 **2.8.5 Release as part of civil discovery**

284 No stipulation.

### 285 **2.8.6 Disclosure upon owner's request**

286 Disclosure upon owner's request is done according to the Data Protection Act  
287 [DPA00], Section 7. Specifically, information is released to the Subscriber  
288 if the CA has received a Signed Email from the Subscriber requesting the  
289 information. The CA charges no fee for this.

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

### 294 **2.8.7 Other information release circumstances**

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

## 297 **2.9 Intellectual Property Rights**

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

299 Parts of this document are inspired by or copied from (in no particular  
300 order) [CFS<sup>+</sup>03], [BG01], [Eur00], [Tru], [NCS99], [FBC99], [Gen01], and  
301 [Cec01].

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

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

## 306 Chapter 3

# 307 IDENTIFICATION AND 308 AUTHENTICATION

### 309 3.1 Initial Registration

#### 310 3.1.1 Types of names

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

314 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.

315  
316 Common Names (CNs) must be encoded as `PrintableStrings` ([WCHK97],[HKYR95]).

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

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

319 ' ', '0' - '9', 'a' - 'z', 'A' - 'Z', '(', ')', '-',

320 that is, Space (blank), decimal digits, lower and upper case US ASCII letters,  
 321 left and right round brackets, and hyphen. For host and service certificates,  
 322 the character '.' (full stop, or period) is also allowed in the Common Name.  
 323 For service certificates, the character '/' is also allowed in the Common Name.

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

328 See also 7.1.4.

### 329 **3.1.2 Need for names to be meaningful**

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

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

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

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

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

### 343 **3.1.3 Rules for interpreting various name forms**

344 No stipulation.

**3.1.4 Uniqueness of names**

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

**3.1.5 Name claim dispute resolution procedure**

No stipulation.

**3.1.6 Recognition, authentication and role of trademarks**

No stipulation.

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

No stipulation.

**3.1.8 Authentication of organisation identity**

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

**3.1.9 Authentication of individual identity**

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

In either case the Subscriber selects which RA is to carry out the identification process.

---

Person	The Subscriber goes to the selected RA Operator bringing acceptable photo ID.
Server	The requestor must <i>either</i> go to the RA Operator in person and prove his/her identity as for personal certificates, and confirm that (s)he is responsible for the resources mentioned in the request, <i>or</i> send Signed Email to the RA Operator confirming the request and confirming that the requestor is responsible for the resources in question.
Service	As server certificates (the person responsible for a host is regarded as the person responsible for all services running on that host).

370 For personal certificates we allow in exceptional cases an “External” ver-  
371 ification for Subscribers who are not able to follow the above procedure for  
372 personal certificates: The Subscriber can send an email confirming the re-  
373 quest to the CA. The request is accepted by the CA if the email is signed by  
374 a certificate from another CA whose certificates are accepted for this purpose  
375 by the CA Manager. The list of such CAs will be decided by the CA Manager  
376 and is available on the CA’s web site [CAW]. In this case, the CN of the  
377 certificate used to sign the email and the CN of the certificate request must  
378 be identical. Subscribers should not use this procedure unless there is no al-  
379 ternative. Subscribers identified through this procedure will have OU=CLRC,  
380 L=External as RA identifier in their certificates.

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

## 383 3.2 Routine Re-key

384 No stipulation.

### 385 **3.3 Re-key After Revocation**

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

### 388 **3.4 Revocation Request**

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

393 Authenticated certificate revocation requests may be made by

- 394 • The RA using:
  - 395 – Signed Email to the CA Manager;
  - 396 – Other secure method, as specified in the RA Operator's procedure.
- 397 • The Subscriber by:
  - 398 – Mailing the CA manager directly by Signed Email.



## 399 Chapter 4

# 400 OPERATIONAL 401 REQUIREMENTS

### 402 4.1 Certificate Application

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

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

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

### 411 4.2 Certificate Issuance

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

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

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

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

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

428 All issued certificates are issued under the CP/CPS valid at the time of  
429 issuance.

### 430 **4.3 Certificate Acceptance**

431 No stipulation.

## 432 **4.4 Certificate Suspension and Revocation**

### 433 **4.4.1 Circumstances for revocation**

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

- 437 • The CA is informed that the Subscriber has ceased to be a member of  
438 or associated with a UK e-Science program or activity;
- 439 • the Subscriber's private key is lost or suspected to be compromised;
- 440 • the information in the subscriber's certificate is wrong or inaccurate,  
441 or suspected to be wrong or inaccurate;
- 442 • the Subscriber violates his/her obligations.

### 443 **4.4.2 Who can request revocation**

444 A certificate revocation can be requested by:

- 445 • The Registration Authority which authenticated the holder of the cer-  
446 tificate;

- 447     • the holder of the certificate;
- 448     • any person presenting proof of knowledge that the subscriber's private
- 449       key has been compromised or that the subscriber's data have changed.

#### 450 **4.4.3 Procedure for revocation request**

451 A revocation request is accepted if:

- 452     • The revocation request is signed with the key corresponding to certifi-
- 453       cate whose revocation is requested; or,
- 454     • The revocation request is signed by the RA who originally approved
- 455       the certificate request.

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

457 revocation is properly authenticated.

#### 458 **4.4.4 Revocation request grace period**

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

460 must request revocation:

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

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

466 the other circumstances for revocation are fulfilled.

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

468 mining the need for revocation.

#### 469 **4.4.5 Circumstances for suspension**

470 The CA does not offer suspension services.

#### 471 **4.4.6 Who can request suspension**

472 No stipulation.

473 **4.4.7 Procedure for suspension request**

474 No stipulation.

475 **4.4.8 Limits on suspension period**

476 No stipulation.

477 **4.4.9 CRL issuance frequency**

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

480 **4.4.10 CRL checking requirements**

481 No stipulation.

482 **4.4.11 On-line revocation/status checking availability**

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

484 **4.4.12 On-line revocation checking requirements**

485 No stipulation.

486 **4.4.13 Other forms of revocation advertisements avail-  
487 able**

488 No stipulation.

489 **4.4.14 Checking requirements for other forms of revo-  
490 cation advertisements**

491 No stipulation.

#### 492 **4.4.15 Special requirements re key compromise**

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

### 497 **4.5 Security Audit Procedures**

#### 498 **4.5.1 Types of event recorded**

499 The following events are recorded:

- 500 • certification requests;
- 501 • issued certificates;
- 502 • requests for revocation;
- 503 • issued CRLs;
- 504 • login/logout/reboot of the signing machine.

#### 505 **4.5.2 Frequency of processing log**

506 No stipulation.

#### 507 **4.5.3 Retention period for audit log**

508 The minimum retention period is 3 years.

#### 509 **4.5.4 Protection of audit log**

510 No stipulation.

#### 511 **4.5.5 Audit log backup procedures**

512 No stipulation.

**513 4.5.6 Audit collection system (internal vs external)**

514 No stipulation.

**515 4.5.7 Notification to event-causing subject**

516 No stipulation.

**517 4.5.8 Vulnerability assessments**

518 No stipulation.

**519 4.6 Records Archival****520 4.6.1 Types of event recorded**

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

- 522 • certification requests;
- 523 • issued certificates;
- 524 • requests for revocation;
- 525 • issued CRLs;
- 526 • all e-mail messages received by the CA (not the confirmation messages  
527 sent to the Subscribers);
- 528 • all e-mail messages sent by the CA;
- 529 • all documents appointing CA and RA Staff.

530 Each RA must log the following:

- 531 • for each approved request, how it was approved;
- 532 • for each rejected request, why it was rejected;
- 533 • for each approved revocation request, the reason for revocation;
- 534 • for each rejected revocation request, the reason for revocation and the  
535 reason the request was rejected.

536 **4.6.2 Retention period for archive**

537 The minimum retention period is 3 years.

538 **4.6.3 Protection of archive**

539 No stipulation.

540 **4.6.4 Archive backup procedures**

541 No stipulation.

542 **4.6.5 Requirements for time-stamping of records**

543 No stipulation.

544 **4.6.6 Archive collection system (internal or external)**

545 No stipulation.

546 **4.6.7 Procedures to obtain and verify archive informa-**  
547 **tion**

548 No stipulation.

549 **4.7 Key Changeover**

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

554 **4.8 Compromise and Disaster Recovery**

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

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

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

#### 563 **4.8.1 Computing resources, software, and/or data are** 564 **corrupted**

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

#### 566 **4.8.2 Entity public key is revoked**

567 No stipulation.

#### 568 **4.8.3 Entity key is compromised**

569 No stipulation.

#### 570 **4.8.4 Secure facility after a natural or other type of** 571 **disaster**

572 No stipulation.

### 573 **4.9 CA Termination**

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

- 575 • inform the Registration Authorities, Subscribers, Relying Parties, and  
576 cross-certifying CAs of which the CA is aware;
- 577 • make information of its termination widely available;
- 578 • stop issuing certificates.

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

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



## 589 Chapter 5

# 590 PHYSICAL, PROCEDURAL, 591 AND PERSONNEL 592 SECURITY CONTROLS

### 593 5.1 Physical Controls

#### 594 5.1.1 Site location and construction

595 No stipulation.

#### 596 5.1.2 Physical access

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

#### 600 5.1.3 Power and air conditioning

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

603 The signing machine is switched off between signing operations. The machine  
604 operates in an air conditioned environment.

605 **5.1.4 Water exposures**

606 No stipulation.

607 **5.1.5 Fire prevention and protection**

608 No stipulation.

609 **5.1.6 Media storage**

610 No stipulation.

611 **5.1.7 Waste disposal**

612 No stipulation.

613 **5.1.8 Off-site backup**

614 No stipulation.

615 **5.2 Procedural Controls**

616 **5.2.1 Trusted roles**

617 No stipulation.

618 **5.2.2 Number of persons required per task**

619 No stipulation.

620 **5.2.3 Identification and authentication for each role**

621 No stipulation.

## 5.3 Personnel Controls

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

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

### 5.3.2 Background check procedures

No stipulation.

652 **5.3.3 Training requirements**

653 No stipulation.

654 **5.3.4 Retraining frequency and requirements**

655 No stipulation.

656 **5.3.5 Job rotation frequency and sequence**

657 No stipulation.

658 **5.3.6 Sanctions for unauthorized actions**

659 In the event of unauthorised actions, abuse of authority or unauthorised use  
660 of entity systems by the CA or RA Operators, the CA manager may revoke  
661 the privileges concerned.

662 **5.3.7 Contracting personnel requirements**

663 No stipulation.

664 **5.3.8 Documentation supplied to personnel**

- 665 • It is the responsibility of the CA Manager to provide the CA Operators  
666 with a copy of the “e-Science CA Operator’s Procedure”.
- 667 • It is the responsibility of the CA Manager to provide the RA Manager  
668 with a copy of the “e-Science RA Manager’s Procedure”.
- 669 • It is the responsibility of the RA Manager to provide the RA Operator  
670 with a copy of the “e-Science RA Operator’s Procedure”.

## 671 Chapter 6

# 672 TECHNICAL SECURITY 673 CONTROLS

## 674 6.1 Key Pair Generation and Installation

### 675 6.1.1 Key pair generation

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

### 678 6.1.2 Private key delivery to entity

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

### 681 6.1.3 Public key delivery to certificate issuer

682 Subscribers' public keys are delivered to the issuing CA by the HTTP pro-  
683 tocol via the CA's web interface.

### 684 6.1.4 CA public key delivery to subscribers

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

### 687 **6.1.5 Key sizes**

688 Keys of length less than 1024 bits are not accepted. The CA key is of length  
689 2048 bits.

### 690 **6.1.6 Public key parameters generation**

691 No stipulation.

### 692 **6.1.7 Parameter quality checking**

693 No stipulation.

### 694 **6.1.8 Hardware/software key generation**

695 No stipulation.

### 696 **6.1.9 Key usage purposes (as per X.509 v3 key usage 697 field)**

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

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

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

## 703 **6.2 Private Key Protection**

### 704 **6.2.1 Standards for cryptographic module**

705 No stipulation.

### 706 **6.2.2 Private key (n out of m) multi-person control**

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

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

### 711 **6.2.3 Private key escrow**

712 Private keys must not be escrowed.

### 713 **6.2.4 Private key backup**

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

### 718 **6.2.5 Private key archival**

719 No stipulation.

### 720 **6.2.6 Private key entry into cryptographic module**

721 No stipulation.

### 722 **6.2.7 Method of activating private key**

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

### 726 **6.2.8 Method of deactivating private key**

727 No stipulation.

### 728 **6.2.9 Method of destroying private key**

729 No stipulation.

## 730 **6.3 Other Aspects of Key Pair Management**

### 731 **6.3.1 Public key archival**

732 The CA archives all issued certificates.

### 733 **6.3.2 Usage periods for the public and private keys**

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

## 736 **6.4 Activation Data**

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

### 738 **6.4.1 Activation data generation and installation**

739 No stipulation.

### 740 **6.4.2 Activation data protection**

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

### 745 **6.4.3 Other aspects of activation data**

746 No stipulation.

## 747 **6.5 Computer Security Controls**

### 748 **6.5.1 Specific computer security technical requirements**

749 The CA server includes the following functionality:

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

### 754 **6.5.2 Computer security rating**

755 No stipulation.

## 756 **6.6 Life-Cycle Technical Controls**

### 757 **6.6.1 System development controls**

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

### 760 **6.6.2 Security management controls**

761 No stipulation.

### 762 **6.6.3 Life cycle security ratings**

763 No stipulation.

## 764 **6.7 Network Security Controls**

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

## 768 **6.8 Cryptographic Module Engineering Con-** 769 **trols**

770 No stipulation.



## 771 Chapter 7

# 772 CERTIFICATE AND CRL 773 PROFILES

### 774 7.1 Certificate Profile

#### 775 7.1.1 Version number

776 X.509.v3

#### 777 7.1.2 Certificate extensions

778 Server and service certificates have the same extensions.

Basic Constraints	<i>critical</i> , CA:FALSE
Key Usage	<i>critical</i> , Digital Signature, Non Repudiation, Key Encryption, Key Agreement
Subject Key Identifier	hash
Authority Key Identifier	keyid, issuer
Subject Alternative Name (server/service only)	Server's Fully Qualified Domain Name

Issuer Name	Alternative	CA email
CRL Points	Distribution	[CAC]
Netscape Cert Type		Personal: SSL Client, S/MIME Server, service: SSL Client, SSL Server
Netscape Comment		“UK e-Science User Certificate”
Netscape CA Revocation URL		[CAC]
Netscape Revocation URL		[CAC]
Netscape URL	Renewal	<a href="http://ca-renew.grid-support.ac.uk/renew.html">http://ca-renew.grid-support.ac.uk/renew.html</a>

779 CA certificate extensions.

Basic Constraints		<i>critical</i> CA:TRUE
Key Usage		keyCertSign, cRLSign
Subject Key Identifier		hash
Authority Key Identifier		keyid, issuer
Subject Name	Alternative	CA email
Issuer Name	Alternative	CA email

CRL Distribution Points	[CAC]
Netscape Cert Type	SSL CA, S/MIME CA

### 780 7.1.3 Algorithm object identifiers

781 No stipulation.

### 782 7.1.4 Name forms

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

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

786 Issuer as seen with OpenSSL version 0.9.7:

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

789 Subject: The subject field contains the Distinguished Name of the entity  
790 with the following attributes:

Country Name	UK
Organisation Name	eScience
Organizational Unit	Name of physical organisation hosting the RA approving the Subject's request
Locality	Location within the organisation where the RA is appointed.
CommonName	Name and surname (personal and object-signing certificates) or DNS name (server certificates). Grid service certificates are prefixed by the service name (see 7.1.5) by / (e.g. CN=ldap/ldap.rl.ac.uk).

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

### 791 **7.1.5 Name constraints**

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

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

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

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

- 801 • the name of the service,
- 802 • the default port number,
- 803 • a short description of the service,
- 804 • a reference URI.

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

### 806 **7.1.6 Certificate policy Object Identifier**

807 No stipulation.

### 808 **7.1.7 Usage of Policy Constraints extensions**

809 No stipulation.

### 810 **7.1.8 Policy qualifier syntax and semantics**

811 No stipulation.

812 **7.1.9 Processing semantics for the critical certificate**  
813 **policy**

814 No stipulation.

815 **7.2 CRL Profile**

816 **7.2.1 Version number**

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

819 **7.2.2 CRL and CRL Entry Extensions**

820 No stipulation.



## 821 Chapter 8

# 822 SPECIFICATION 823 ADMINISTRATION

### 824 8.1 Specification Change Procedures

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

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

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

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

838 *Security updates:* changes that affect the security, e.g. changes to the minimal  
839 requirements for verifying requests, or changing the key sizes. These changes  
840 will be announced at least 30 days in advance on the CA web site, and to  
841 appropriate mailing lists, including the DataGrid CA mailing list. However,  
842 urgent security fixes may be carried out without advance warning and then  
843 documented in the CPS. These will be announced in the same manner.

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

846 web site and appropriate mailing lists.

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

## 849 **8.2 Publication and Notification Policies**

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

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

## 856 **8.3 CPS Approval Procedures**

857 No stipulation.

# 858 Appendix A

## 859 Revision History

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.
1.0	1.4	30 October 2003	Describe renewal. Tightened up several parts, including Applicability, personal information stored, etc.
1.1	1.5		More about the data protection act.

860

<sup>861</sup> The OID in the table is the final two digits of the actual OID, as defined in  
<sup>862</sup> section 1.2.

## 863 Bibliography

- 864 [BG01] Randy Butler and Tony Genovese. Global grid forum certificate  
865 policy model. [http://www.gridforum.org/2\\_SEC/pdf/Draft-  
GGF-CP-06.pdf](http://www.gridforum.org/2_SEC/pdf/Draft-<br/>866 GGF-CP-06.pdf), September 2001.
- 867 [CAC] CA Certificate Revocation List. [http://ca.grid-support.ac.uk/-  
cgi-bin/importCRL](http://ca.grid-support.ac.uk/-<br/>868 cgi-bin/importCRL).
- 869 [CAW] CA web site. <http://www.grid-support.ac.uk/ca/>.
- 870 [Cec01] R. Cecchini. INFN CA CP/CPS. [http://security.fi.infn.it/CA/-  
CPS/CPS-1.0.pdf](http://security.fi.infn.it/CA/-<br/>871 CPS/CPS-1.0.pdf), December 2001. Version 1.0.
- 872 [CF99] S. Chokani and W. Ford. Internet X.509 Infrastruc-  
873 ture Certificate Policy and Certification Practices Framework.  
874 <http://www.rfc-editor.org/rfc/rfc2527.txt>, March 1999.
- 875 [CFS<sup>+</sup>03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet  
876 x.509 public key infrastructure certificate policy and certification  
877 practices framework. [http://www.ietf.org/internet-drafts/draft-  
ietf-pkix-ipki-new-rfc2527-02.txt](http://www.ietf.org/internet-drafts/draft-<br/>878 ietf-pkix-ipki-new-rfc2527-02.txt), April 2003.
- 879 [DPA00] Data protection act 1998. [http://www.legislation.hmso.gov.uk/-  
acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/-<br/>880 acts/acts1998/19980029.htm), March 2000.
- 881 [Eur00] EuroPKI Certificate Policy. [http://www.europki.org/ca/root/-  
cps/en\\_cp.pdf](http://www.europki.org/ca/root/-<br/>882 cps/en_cp.pdf), October 2000. Version 1.1.
- 883 [FBC99] X.509 Certificate Policy For The Federal Bridge Certification Au-  
884 thority. Available from <http://www.cio.gov/fbca/lib/index.htm>,  
885 December 1999. Version 1.0.
- 886 [Gen01] Tony Genovese. DOE Science Grid CA CP/CPS.  
887 <http://www.doegrids.org/Docs/CP-CPS.pdf>, December 2001.  
888 Version 1.1.

- 889 [Gloa] Globus. Grid security infrastructure for globus toolkit 2.  
890 <http://www.globus.org/security/v2.0/index.html>.
- 891 [Glob] Globus. Grid security infrastructure for globus toolkit 3.  
892 <http://www.globus.org/security/GSI3/index.html>.
- 893 [GSC] UK Grid Support Centre. <http://www.grid-support.ac.uk/>.
- 894 [HKYR95] T. Howes, S. Kille, W. Yeung, and C. Robbins. The String  
895 Representation of Standard Attribute Syntaxes. <http://www.rfc-editor.org/rfc/rfc1778.txt>, March 1995.  
896
- 897 [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public  
898 key infrastructure certificate and certificate revocation list (crl)  
899 profile. <http://www.rfc-editor.org/rfc/rfc3280.txt>, April 2002.
- 900 [IAN] Port numbers. <http://www.iana.org/assignments/port-numbers>.
- 901 [NCS99] National Computational Science Alliance Certificate Pol-  
902 icy. [http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html)  
903 [Certificates/AllianceCP9.1.html](http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html), June 1999.
- 904 [Tru] TrustID Certificate Policy. [http://www.digsigtrust.com/-](http://www.digsigtrust.com/-certificates/policy/tsindex.html)  
905 [certificates/policy/tsindex.html](http://www.digsigtrust.com/-certificates/policy/tsindex.html).
- 906 [WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight  
907 Directory Access Protocol (v3): Attribute Syntax Definitions.  
908 <http://www.rfc-editor.org/rfc/rfc2252.txt>, December 1997.