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

Jens G Jensen

CCLRC

Rutherford Appleton Laboratory

04 March 2005

Contents

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 04 March 2005 and took effect on 04 March 2005.

1.1.1 General definitions

The document makes use of the following terms:

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

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

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

Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, the issuing CA is the CA that issued the certificate.
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 *not encrypted*, (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).

1.2 Identification

Document title	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
Document version	Version 1.1
Document date	04 March 2005
Effective from	04 March 2005
Document OID	1.3.6.1.4.1.11439.1.1.1.1.5

The document OID is {`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) cclrc(11439) 1 escience(1) ca(1) cps(1) 5`}.

See also revision history in Appendix A.

1.3 Community and Applicability

1.3.1 Certification authorities

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

1.3.2 Registration authorities

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

1.3.3 End entities (Subscribers)

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

1.3.4 Applicability

Certificates issued are suitable for the following applications:

- SSL or GSI client (all certificates);
- SSL or GSI server (server and service certificates only);
- GSI service (service certificates only);
- Generating GSI proxies (all certificates);

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

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

1.4 Contact Details

1.4.1 Specification administration organisation

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

1.4.2 Contact person

The CA manager (contact person for questions related to this policy document) is:

```
Dr Jens G Jensen
Rutherford Appleton Laboratory
Chilton
Didcot
Oxon
OX11 0QX
UK

Phone: +44 1 235 446104
Fax:   +44 1 235 445945
Email:   ca-manager@grid-support.ac.uk
```

1.4.3 Person determining CPS suitability for the policy

The person mentioned in 1.4.2.

Chapter 2

GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The CA must:

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

2.1.2 RA obligations

The RA Manager must:

- agree the name of the RA (the values of the `OU` and `L` in the DN) with the CA Manager;
- define the community of Subscribers for which the RA will approve requests, and any requirements in addition to those imposed by this CP/CPS;
- ensure that (s)he is appointed according to the procedures described in this CP/CPS;
- appoint one or more RA Operators according to the procedures described in this CP/CPS;
- ensure that the Operator(s) operate according to the procedures provided by the CA;
- in particular, ensure that the RA stores all logs and additional Subscriber information securely, and is released only according to the conditions described in section 2.8;
- provide access to the logs when requested by the CA.

The RA Operator must:

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

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

2.1.3 Subscriber obligations

Subscribers must:

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

2.1.4 Relying party obligations

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

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

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

2.1.5 Repository obligations

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

2.2 Liability

2.2.1 CA liability

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

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

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

2.2.2 RA liability

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

2.3 Financial Responsibility

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

2.3.1 Indemnification by relying parties

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

No stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing law

Interpretation of this policy is according to UK Law.

2.4.2 Severability, survival, merger, notice

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

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

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

2.4.3 Dispute resolution procedures

No stipulation.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

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

2.5.2 Certificate access fees

No fees are charged for certificate access.

2.5.3 Revocation or status information access fees

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

2.5.4 Fees for other services such as policy information

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

2.5.5 Refund policy

No stipulation.

2.6 Publication and Repositories

2.6.1 Publication of CA information

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

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

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

2.6.2 Frequency of publication

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

2.6.3 Access controls

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

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

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

2.6.4 Repositories

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

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

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

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

2.7.2 Identity/qualifications of auditor

No stipulation.

2.7.3 Auditor's relationship to audited party

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

2.7.4 Topics covered by audit

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

2.7.5 Actions taken as a result of deficiency

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

2.7.6 Communication of results

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

2.8 Confidentiality

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

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

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

2.8.1 Types of information to be kept confidential

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

2.8.2 Types of information not considered confidential

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

Statistics regarding certificates issuance and revocation contain no personal information and is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

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

2.8.4 Release to law enforcement officials

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

2.8.5 Release as part of civil discovery

No stipulation.

2.8.6 Disclosure upon owner's request

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

The CA will recognise requests in writing for the release of personal information from a Subscriber provided the Subscriber can be properly authenticated. The CA reserves the right to charge a reasonable fee for the service in this case.

2.8.7 Other information release circumstances

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

2.9 Intellectual Property Rights

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

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

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

This document typeset with LaTeX.

Chapter 3

IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

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

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.

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

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

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

Email address in server and service certificates must be structured according to RFC822. The maximal length of an email address is 128 characters. Email addresses must be encoded as `IA5String` but most not contain control characters or delete.

See also 7.1.4.

3.1.2 Need for names to be meaningful

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.

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

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

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

3.1.3 Rules for interpreting various name forms

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 *either* 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, *or* 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).

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

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

3.2 Routine Re-key

No stipulation.

3.3 Re-key After Revocation

There is no re-key after revocation. Subscribers must apply for a new certificate.

3.4 Revocation Request

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

Authenticated certificate revocation requests may be made by

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

Chapter 4

OPERATIONAL REQUIREMENTS

4.1 Certificate Application

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

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

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

4.2 Certificate Issuance

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

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

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

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

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

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

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

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

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

4.4.2 Who can request revocation

A certificate revocation can be requested by:

- The Registration Authority which authenticated the holder of the certificate;

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

4.4.3 Procedure for revocation request

A revocation request is accepted if:

- The revocation request is signed with the key corresponding to certificate whose revocation is requested; or,
- The revocation request is signed by the RA who originally approved the certificate request.

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

4.4.4 Revocation request grace period

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

- immediately using the online revocation facilities, if (s)he still has access to the private key;
- otherwise by going to the RA as soon as possible and ask the RA to request revocation.

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

The revocation will take place within one working day of the CA determining the need for revocation.

4.4.5 Circumstances for suspension

The CA does not offer suspension services.

4.4.6 Who can request suspension

No stipulation.

4.4.7 Procedure for suspension request

No stipulation.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency

CRLs are updated and re-issued within one hour after every certificate revocation or at least every week.

4.4.10 CRL checking requirements

No stipulation.

4.4.11 On-line revocation/status checking availability

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

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.15 Special requirements re key compromise

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

4.5 Security Audit Procedures

4.5.1 Types of event recorded

The following events are recorded:

- certification requests;
- issued certificates;
- requests for revocation;
- issued CRLs;
- login/logout/reboot of the signing machine.

4.5.2 Frequency of processing log

No stipulation.

4.5.3 Retention period for audit log

The minimum retention period is 3 years.

4.5.4 Protection of audit log

No stipulation.

4.5.5 Audit log backup procedures

No stipulation.

4.5.6 Audit collection system (internal vs external)

No stipulation.

4.5.7 Notification to event-causing subject

No stipulation.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of event recorded

The following events are recorded and archived by the CA:

- certification requests;
- issued certificates;
- requests for revocation;
- issued CRLs;
- all e-mail messages received by the CA (not the confirmation messages sent to the Subscribers);
- all e-mail messages sent by the CA;
- all documents appointing CA and RA Staff.

Each RA must log the following:

- for each approved request, how it was approved;
- for each rejected request, why it was rejected;
- for each approved revocation request, the reason for revocation;
- for each rejected revocation request, the reason for revocation and the reason the request was rejected.

4.6.2 Retention period for archive

The minimum retention period is 3 years.

4.6.3 Protection of archive

No stipulation.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

No stipulation.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key Changeover

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

4.8 Compromise and Disaster Recovery

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

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

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

4.8.1 Computing resources, software, and/or data are corrupted

The CA will take best effort precautions to enable recovery.

4.8.2 Entity public key is revoked

No stipulation.

4.8.3 Entity key is compromised

No stipulation.

4.8.4 Secure facility after a natural or other type of disaster

No stipulation.

4.9 CA Termination

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

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

An advance notice of no less than 60 days will be given in the case of normal (scheduled) termination. The CA Manager at the time of termination shall be responsible for the subsequent archival of all records as required in section 4.6.2.

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

Chapter 5

PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

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

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

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.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

- It is the responsibility of the CA Manager to provide the CA Operators with a copy of the "e-Science CA Operator's Procedure".
- It is the responsibility of the CA Manager to provide the RA Manager with a copy of the "e-Science RA Manager's Procedure".
- It is the responsibility of the RA Manager to provide the RA Operator with a copy of the "e-Science RA Operator's Procedure".

Chapter 6

TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

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

6.1.2 Private key delivery to entity

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

6.1.3 Public key delivery to certificate issuer

Subscribers' public keys are delivered to the issuing CA by the HTTP protocol via the CA's web interface.

6.1.4 CA public key delivery to subscribers

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

6.1.5 Key sizes

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

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

No stipulation.

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

Keys may be used for authentication, non-repudiation, data encryption, message integrity and session key establishment.

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

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

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

No stipulation.

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

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

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

6.2.3 Private key escrow

Private keys must not be escrowed.

6.2.4 Private key backup

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

6.2.5 Private key archival

No stipulation.

6.2.6 Private key entry into cryptographic module

No stipulation.

6.2.7 Method of activating private key

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

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The CA archives all issued certificates.

6.3.2 Usage periods for the public and private keys

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

6.4 Activation Data

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

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The CA server includes the following functionality:

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

6.5.2 Computer security rating

No stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System development controls

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

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

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

6.8 Cryptographic Module Engineering Controls

No stipulation.

Chapter 7

CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number

X.509.v3

7.1.2 Certificate extensions

Server and service certificates have the same extensions.

Basic Constraints	*critical*, CA:FALSE
Key Usage	*critical*, 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 Alternative Name	CA email
CRL Distribution Points	[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 Renewal URL	http://ca-renew.grid-support.ac.uk/renew.html
Signature Algorithm	sha1WithRSAEncryption

779 CA certificate extensions.

Basic Constraints	*critical* CA:TRUE
Key Usage	*critical* keyCertSign, cRLSign
Subject Key Identifier	hash
Authority Key Identifier	keyid, issuer
Subject Alternative Name	CA email

Issuer Alternative Name	CA email
CRL Distribution Points	[CAC]
Netscape Cert Type	SSL CA, S/MIME CA
Signature Algorithm	sha1WithRSAEncryption

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

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

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

Issuer as seen with OpenSSL version 0.9.7:

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

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

7.1.5 Name constraints

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

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

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

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

- the name of the service,
- the default port number,
- a short description of the service,
- a reference URI.

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

7.1.6 Certificate policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints extensions

No stipulation.

7.1.8 Policy qualifier syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy

No stipulation.

7.2 CRL Profile

7.2.1 Version number

X.509.v1: Version 1 is required for compatibility with Netscape Communicator.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

Chapter 8

SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

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

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

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

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

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

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

web site and appropriate mailing lists.

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

8.2 Publication and Notification Policies

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

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

8.3 CPS Approval Procedures

No stipulation.

Appendix A

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	04 March 2005	Documented that we use SHA1 to sign.

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

Bibliography

[BG01] Randy Butler and Tony Genovese. Global grid forum certificate policy model. http://www.gridforum.org/2_SEC/pdf/Draft-GGF-CP-06.pdf, September 2001.

[CAC] CA Certificate Revocation List. http://ca.grid-support.ac.uk/-cgi-bin/importCRL.

[CAW] CA web site. http://www.grid-support.ac.uk/ca/.

[Cec01] R. Cecchini. INFN CA CP/CPS. http://security.fi.infn.it/CA/-CPS/CPS-1.0.pdf, December 2001. Version 1.0.

[CF99] S. Chokani and W. Ford. Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework. http://www.rfc-editor.org/rfc/rfc2527.txt, March 1999.

[CFS+03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet x.509 public key infrastructure certificate policy and certification practices framework. http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-02.txt, April 2003.

[DPA00] Data protection act 1998. http://www.legislation.hmso.gov.uk/-acts/acts1998/19980029.htm, March 2000.

[Eur00] EuroPKI Certificate Policy. http://www.europki.org/ca/root/-cps/en_cp.pdf, October 2000. Version 1.1.

[FBC99] X.509 Certificate Policy For The Federal Bridge Certification Authority. Available from http://www.cio.gov/fbca/lib/index.htm, December 1999. Version 1.0.

[Gen01] Tony Genovese. DOE Science Grid CA CP/CPS. http://www.doegrids.org/Docs/CP-CPS.pdf, December 2001. Version 1.1.

[Gloa] Globus. Grid security infrastructure for globus toolkit 2. http://www.globus.org/security/v2.0/index.html.

[Glob] Globus. Grid security infrastructure for globus toolkit 3. http://www.globus.org/security/GSI3/index.html.

[GSC] UK Grid Support Centre. http://www.grid-support.ac.uk/.

[HKYR95] T. Howes, S. Kille, W. Yeoung, and C. Robbins. The String Representation of Standard Attribute Syntaxes. http://www.rfc-editor.org/rfc/rfc1778.txt, March 1995.

[HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. http://www.rfc-editor.org/rfc/rfc3280.txt, April 2002.

[IAN] Port numbers. http://www.iana.org/assignments/port-numbers.

[NCS99] National Computational Science Alliance Certificate Policy. http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/-Certificates/AllianceCP9.1.html, June 1999.

[Tru] TrustID Certificate Policy. http://www.digsigtrust.com/-certificates/policy/tsindex.html.

[WCHK97] M. Wahl, A. Coulbeck, T. Howes, and S. Kille. Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions. http://www.rfc-editor.org/rfc/rfc2252.txt, December 1997.