UK e-Science Root Certificate Policy and Certification Practices Statement

Jens Jensen
CCLRC
Rutherford Appleton Laboratory

14 Jul 2006

1 Introductions

This document is the Certificate Policy and Certification Practices Statement for the UK e-Science Root CA. The root issues CA certificates for Grid and e-Science work in the UK.

This document is structured according to RFC 3647. It is typeset with LaTeX.

1.1 Overview

The e-Science Root issues certificates to CAs in UK e-Science, and in particular it shall issue and maintain a CA certificate as a Subject CA for the "classic" medium assurance e-Science CA which in turn is used to identify persons and host/services.

The Root CA shall provide publicly available documentation on its web site of the current and past structure of its PKI, throughout its lifetime.

The purpose of the Root CA is:

- To define and limit the community that Subordinate CAs may serve;
- To ensure that Subordinate CAs with different assurance levels and purposes can coexist;

  > Rationale: For example, it is necessary to ensure that all Subordinate CAs issue in distinct namespaces because many RPs only check the Subject DN for authorisation purposes.

- To enable Subordinate CAs to be maintained in adequately protected networked systems, according to their policy and purpose.

  > Rationale: A Subordinate CA's certificate can relatively easily be revoked and reissued, whereas revoking and reissuing a root is more harmful to the PKI.

1.2 Document Name and Identification

This document is the CP and CPS of the UK e-Science Root CA. It was issued on 26 May 2006, and took effect on 14 July 2006.

The OID of this document is {`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) cclrc(11439) 1 escience(1) rootca(2) cps(1) 1`}.

1.3 PKI Participants

- Certification Authorities: The e-Science Root CA only issues CA certificates. Subject CAs under the Root may themselves issue to further Subordinate CAs.
- Registration Authorities: There are no RAs external to the issuing authority. The issuing authority alone is responsible for all approvals and revocations.
- Subscribers: Only Subject CAs receive certificates from the Root.
- Relying Parties: no stipulation.

1.4 Certificate Usage

The Root certificate may be used for the following purpose:

- To validate the signature of a Subject CA; and, more generally, as a part of validation of any certificate chain ending with the Root, provided all certificates in the chain are being used for their permitted purposes;
- To validate the signature on a CRL issued by the Root.

No other use of the e-Science root is permitted.

Nothing should be inferred about the assurance of Subordinate CAs: they may have different assurance levels and purposes, and the Root does not guarantee a minimum. RPs should consult the policy of Subordinate CAs before reliance. The Root does assert that all Subordinate CAs serve the same community, and they all issue in distinct namespaces – see section 3.1.

1.5 Policy Administration

The organisation responsible for this CA is the Council for the Central Laboratory of the Research Councils (CCLRC).

The person responsible for this policy and the practices of the CA is:


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

Tel: +44 1235 446104
Fax: +44 1235 445945
Email: j.jensen@rl.ac.uk
```

1.6 Definitions and Acronyms

- CCLRC is the Council for the Central Laboratories of the Research Council, one of the UK research councils.
- For the purposes of this document, a **Subject CA** is a CA whose certificate was issued by the Root whose policy and practices are described in this document;
- For the purposes of this document, a **Subordinate CA** is a Subject CA *or any CA underneath it.* In other words, a Subordinate CA is a CA anywhere in the hierarchy whose root is described in this document.
- For the purposes of this document, **Profile** refers to the content of the signed envelope within a certificate, but excluding the public key itself and the lifetime. Thus, Profile normally comprises extensions, the issuer and subject names, but also the type of keys and algorithms, and the version of the certificate.

2 Publication and Repository Responsibilities

It is the responsibility of the Root CA to publish the following information:

- Its CP/CPS;
- Its certificate;
- All certificates issued by the CA and their status;
- An overview of the hierarchy of which it forms the root;
- Its CRL.

3 Identification and Authentication

3.1 Naming

- Each of the Subject CAs shall have a unique name;
- The Subject name of each Subject CA shall be formed so that the written form starts with `/C=UK/O=eScience`*XXX*`/`.
- Here, *XXX* denotes a string which shall have some basic relation to the purpose of the Subject CA, sufficient to enable a person familiar with the hierarchy to distinguish the Subject CAs from each other by their Subject DN alone;
- Each Subordinate CA shall be named in a scheme which enables a person familiar with the hierarchy to distinguish whether a Subordinate CA is a Subject CA or not, by their Subject DN alone;
- All Subordinate CAs shall issue certificates in mutually independent namespaces;
- No subject name of a Subject CA shall be reused anywhere in the hierarchy.

3.2 Initial Identity Validation

A certificate shall be issued to a Subject CA only when

- The Subject CA has defined CP and CPS consistent with the policy and practices described in this document;
- The Subject CA has implemented and described policy and practices sufficient to meet the restrictions that this document imposes on Subject CAs and all Subordinate CAs issued under the Subject CA;
- The Subject CA has submitted a certificate request and is able to prove to the Root CA possession of the corresponding private key;

Furthermore, the Root CA requires, as a condition for certificate issuance, that:

- All Subject CAs make available to the Root CA results of CA audits and plans to remedy deficiencies;
- All Subject CA Managers and Operators agree to be signed up to a closed mailing list, maintained by the Root CA;
- The Subject CA's certificate request (and hence certificate) contains no personal information.

3.3 Identification and Authentication for Re-key Requests

The CA Manager of the Subject CA shall prove possession of the private key corresponding to the certificate being renewed, and prove possession of the private key corresponding to the request being submitted.

3.4 Identification and Authentication for Revocation Requests

The certificate of a Subject CA will be revoked when:

- A revocation request is received which is signed with the private key of the Subject CA; or,
- An authenticated revocation request from the CA Manager of the Subject CA is received; or
- The Root CA has otherwise determined the need for revocation, e.g., if the Subject CA does not comply with the requirements imposed on it by the Root.

4 Certificate Life-Cycle Operational Requirements

For both Root CA and Subject CAs, keys shall be generated by the CA Manager, using high entropy input. The private key shall be protected according to the practices of the CA.

The Subject CA certificate shall have a lifetime not exceeding five years. The Root CA's certificate shall have a lifetime of twenty years.

4.1 Certificate Application

For an initial request, the Manager of the Subject CA shall agree the namespace of the Subject CA with the Manager of the Root CA, and shall then submit the CP/CPS under which the Subject CA will operate. It is the responsibility of the Manager of the Subject CA to ensure that the Subject CA and all its Subordinate CAs (if any) operate within the constraints imposed by the Policy of the Root.

The Manager of the Subject CA is responsible for the generation of keys for the Subject CA. The Root CA shall not have access to the private key of the Subject CA. The CA Manager of the Subject CA shall submit the request physically (e.g., memory stick, floppy disk) to the Root CA.

4.2 Certificate Application Processing

When the CA Manager of the Root CA is satisfied that the Subject CA and all its Subordinate CAs will operate within the constraints imposed by the Root, the Root CA will issue and publish the certificate of the Subject CA.

4.3 Certificate Issuance

The Root CA makes the Subject CA certificate available on its web site, and notifies the Manager of the Subject CA by phone or mail or otherwise that the certificate has been issued.

4.4 Certificate Acceptance

The CA Manager of the Subject CA shall verify the content of the Subject CA certificate against the CP/CPS of the Subject CA. If the CA Manager of the Subject CA has not made objections to the content of the certificate within five working days, it shall be considered accepted.

In case of non-acceptance, the CA Manager of the Subject CA shall inform the CA Manager of the Root CA, describing required amendments. The certificate shall be revoked by the Root CA, and reissued with the amendments, provided the amended certificate is still compatible with the CP/CPSes of both the Root and Subject CAs. Reissuance may be based on the original request.

> Rationale: The CA Manager of the Subject CA may wish to test the certificate with applicable middleware.

4.5 Key Pair and Certificate Usage

The certificates of all Subordinate CAs and those of the EEs issued by Subordinate CAs must be used only for purposes of direct e-Science and Grid work, or incidental (infrastructure, email).

The certificates issued to Subject CAs may only be used as CA certificates, i.e., for validating certificates issued by them, and for validating CRLs.

A Subordinate CA may impose further constraints on the use of certificates on, and only on, CAs Subordinate to itself and their EEs. Conversely, no Subordinate CA shall relax constraints imposed on its policy or operations by the CP/CPS of a CA of which it is itself Subordinate.

It is the responsibility of the EE to use certificates for permitted purposes only. It is the responsibility of RPs to validate the certificate to their satisfaction at the time of reliance.

4.6 Certificate Renewal

No Subject CA certificate shall be renewed except for the reissuance associated with the non-acceptance of an issued certificate.

4.7 Certificate Re-key

It is the responsibility of the CA Manager of each Subject CA to ensure that a timely rekeying of the Subject CA certificate is requested. The Manager shall further take into account time required for the Root to perform any necessary validations of the Subject CA, operational requirements (Root operator availability and schedule), and the time permitted to the Manager to validate acceptance of the certificate, and certificate redistribution to repositories and RPs.

It is the Manager's responsibility to ensure that this process is complete within a time interval not less than the maximal lifetime of certificates directly issued by the Subject CA before the date of expiry of the Subject CA certificate.

The lifetime of the rekeyed Subject CA certificate shall not exceed that of the Root. It is the responsibility of the CA Manager of the Root CA to ensure that a timely rollover of the Root certificate is in place. To this end, the Root shall require that no Subject CA has a lifetime longer than five years.

The process for acceptance of a rekeyed Subject CA certificate is the same as for the acceptance of an initial request – see section 4.4.

4.8 Certificate Modification

The CA Manager of a Subject CA may request certificate modification. Provided it is consistent with the policy and practices of the Root, the Root shall:

- Reissue the certificate with the requested modifications, provided a timely request is made due to non-acceptance of an issued certificate;
- Issue and re-publish the certificate with the requested modifications based on a new certificate request, as for rekey.

Only in exceptional circumstances will the Root otherwise reissue the certificate with the same keys. The CA Manager of the Subject CA shall describe:

- The need for the modification of the existing certificate;
- Justify the urgency requiring a modified certificate containing the same keys;
- The means by which the modified certificate shall be published and redistributed;
- Compatibility: that the modifications will not impair the usability of the certificate with existing middleware and infrastructure, except to the extent that such impairment is the intention of the modification.

These exceptional circumstances include, but are not limited to:

- Vulnerabilities of cryptographic algorithms used in the certificate are discovered, and a compatible security update is available;
- Exceptional circumstances (force majeure) beyond the control of the CA Manager of the Subject CA has prevented a timely rekeying request, thus requiring a temporary, limited extension of the lifetime of the certificate.

4.9 Certificate Revocation and Suspension

A Subject key CA shall be revoked if:

- It is seen to consistently and wilfully violate its own CP/CPS, or that the CA Manager of the Subject CA does not take steps to address such violations; or,
- It is seen to violate the requirements imposed on it by the policy and practices of the Root; or
- It can be shown that the private key has been compromised

4.10 Certificate Status Services

The Root CA shall issue a CRL. Certificates and certificate status of Subject CAs are available on the Root CA's web site. See also section 7.2.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

The Root shall have no key escrow, nor shall it impose any such on any Subordinate CA. Subordinate CAs may have key escrow.

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

The machine on which the Root signs its certificates and CRLs is kept offline, and is powered down and locked in a safe when not used.

The safe itself is kept in a secure room with logged access control. Trusted non-CA staff may have access to the room but they will not have a key to the safe.

5.2 Procedural Controls

Only Root CA operators are system administrators of the signing machine. Administrative tasks may be performed by any one operator.

For auditing of the signing system (logs), at least one operator must be present.

5.3 Personnel Security Controls

Training: the Root CA is OpenSSL based, and Operators must have sufficient experience with OpenSSL to be able to issue certificates and CRLs. Operators must be permanent members of staff at CCLRC.

5.4 Audit Logging Procedures

All operations on the signing machine are logged, both on paper, and basic system logs on the signing machine itself: bootup/shutdown, login, signatures.

5.5 Records Archival

Records are kept throughout the lifetime of the CA, and for a period no less than three years after the termination of the CA.

5.6 Key Changeover

At re-keying, the new Root keys shall be published on the Root CA's web site, as certificates signed by both the old and the new private key. The transitional certificate, signed with the old key, shall expire at the same time as the old Root certificate, but shall otherwise have the same content as the new Root certificate. It shall be clearly marked as a transitional certificate, and instructions shall be provided for users explaining how to verify the transition.

5.7 Compromise and Disaster Recovery

Following a compromise of the Root private key, the Root CA shall make this widely known to all peer CAs, Subject CAs, and RPs. Subject CAs shall further communicate this to their communities.

5.8 CA or RA Termination

Upon termination of the Root CA, the CA Manager shall communicate this in advance to peer CAs, Subject CAs, and RPs. The advance notice should be no less than the longest lifetime of any currently valid Subject CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

The Root CA's key pair shall be generated with sufficient entropy: every bit of random input comes from a good random source. It shall be the responsibility of the CA Manager to generate the key pair. The Root key pair shall be RSA and have a length of at least 2048 bits.

For Subject CAs, it is the responsibility of the CA Manager to ensure that the key pairs are generated according to best practices. Each Subject CA key pair should have a length of at least 2048 bits.

6.2 Private Key Protection and Cryptographic Module Engineering

The private key of the Root CA shall be protected with with 2-out-of-3 activation data as described in section 6.4. There shall be at any given time exactly three operators.

The private key is not escrowed.

At least three different digital copies of the encrypted private key shall be kept. The digital backups shall have the following properties:

- They shall be kept on at least three different media (e.g., disk, memory stick, tape);

  > RATIONALE: Several different formats are unlikely to go bad, or have drivers fail or become obsolete or unsupported, at the same time.

- They shall be kept so only operators have normal authorised access to them;
- Non-removable media shall be administrated and have access control equivalent to the site's protection of personnel records or their backups;

  > RATIONALE: This implies that encrypted keys can be kept on systems maintained by trusted system administrators. This is required because it greatly improves the quality of storage available.

- Removable media shall be kept locked up, but not in the safe containing the signing machine. No person other than the operator(s) and site operations personnel shall have keys;
- Each copy shall be checked for integrity at least once every year.

The private key must be unencrypted only in volatile memory. The passphrase is typed in as needed, and is also never written to non-volatile storage. The machine used for signing is powered down after the signing.

It is the responsibility of the Operator to safeguard their own copies of the encrypted private key, to take no unauthorised copies thereof, and to surrender all copies to the CA Manager when they cease to be Operators.

Additionally, a printout on paper of the encrypted private key shall be kept in tamper evident envelope in CCLRC's safe for classified information.

6.3 Other Aspects of Key Pair Management

All Root CA certificates shall be kept and published throughout the lifetime of the CA, and a period no less than three years after the termination of the CA.

Subject CAs' key pairs shall have a lifetime not exceeding five years.

6.4 Activation Data

The activation data shall be chosen such that according to current cryptographic practice, estimates, and recommendations, recovering the key from its encrypted form is at least as hard as recovering it from the public key.

The activation data shall then be encoded into ASCII characters as a passphrase. The passphrase shall then be split into three parts, as close to equal length as

possible. These parts are written on paper, and are further referred to in this section as parts A, B, and C.

Each Operator shall be given to parts: Operator 1 gets parts A and B, Operator 2 gets A and C, and Operator 3 gets B and C. Thus, no single Operator, and any two Operators together, have parts A, B, and C. Operators are responsible for the safe keeping of the parts, and, in particular, shall not share them with each other. They are further responsible for not taking copies of them, and for surrendering them to the CA Manager when they cease to be Operators. An Operator may keep the two parts together, but must not keep them in the same location as any copy of the encrypted private key.

Additionally, a full paper copy of the activation data shall be kept in tamper evident envelope in CCLRC's safe for classified information.

The circumstances for updating the activation data include:

- Cryptographic advances have made the encrypted private key vulnerable to attack in the sense that recovering the private key from the encrypted form is significantly easier than recovering it from the public key;
- An Operator is suspected to have copied activation data or shared it with anyone else, or made unauthorised copies of the private key;
- An operator has lost copies of the private key, or of the parts of the passphrase.

The procedure for generating or updating the activation data is as follows:

- (Update only) Operators shall surrender to the CA Manager all copies of the encrypted private key and activation data with the old encryption;
- Together, Operators shall generate new activation data of a sufficient quality as described above, and split it as described above. A brief exposure to other parts of it is not considered a compromise as each part will be too complex to memorise.
- All copies of the previous encrypted private key shall be deleted and replaced with the new version, except the ones in the safe for classified information which may be kept for archival and recovery purposes.

6.5 Computer Security Controls

The signing machine is kept in a safe. There is no other part of the CA other than its web site, whose security controls need not be described in this document.

6.6 Life Cycle Security Controls

Not applicable; see section 6.5.

6.7 Network Security Controls

Not applicable; see section 6.5.

6.8 Time-stamping

The signing machine's clock shall be checked and set every time it is booted up. It is considered sufficient that it is accurate to within one minute.

7 Certificate and CRL Profiles

7.1 Certificate Profile

The Root CA certificate shall have the following Profile:

- The certificate shall be version 3 (i.e., the version number shall be 2);
- The issuer name and subject name shall both be the following:

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

- The signature algorithm shall be `sha1WithRSAEncryption`;
- The extensions shall contain:
  - `basicConstraints`: CA=true, critical;
  - `keyUsage`: certificate signing, CRL signing, critical;
  - There shall be a `subjectKeyIdentifier` and a `authorityKeyIdentifier`; both shall have the hash as a value;
  - CRL distribution points.

The requirements on the Profile of the Subject CAs are as follows:

- They shall be version 3 (i.e., the version number shall be 2);
- `basicConstraints` must be present and be critical and must contain CA=true (but may contain other constraints);
- `keyUsage` must be present and be critical and must have certificate signing and CRL signing set, and no other value;
- They should have `authorityKeyIdentifier` and `subjectKeyIdentifier`, both containing the hash.

Subject CA certificates may contain other extensions.

7.2 CRL Profile

The Root CA issues CRL version 1. The "lifetime" of the CRL is 18 months; and it is issued at least once every year.

7.3 OCSP Profile

Not applicable.

8 Compliance Audit and Other Assessment

A compliance audit shall be carried out by the Root CA once every year, by the Operators. The audit shall inspect the logs, and check the security of the activation data and the copies of the encrypted private key.

9 Other Business and Legal Matters

The section headers in section 9 are taken from RFC3647 and are kept as-is for ease of reference and comparison with other CAs. They must not be interpreted or construed in any way that will affect the intepretation or construction of the contents of the sections.

Certificates and all other components of the CA must be used for lawful purposes only.

Operators shall sign a document to the effect that they will comply with the procedures and requirements described in this document.

9.1 Fees

The Root CA charges no fees for its services.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

Regarding the Freedom of Information (FOI) Act 2000, the Root CA is operated by CCLRC, and the FOI policy of CCLRC applies. Any FOI request must be made to CCLRC.

9.4 Privacy of Personal Information

The Root CA does not process any personal data, except for the following:

- The contact details of the Managers of the Root CA and Subject CA. These are published in the respective CP/CPS documents, and is thus not considered confidential, but they are not published by the Root CA. They must, however, be published by the Subject CAs themselves.
- The email addresses of the Subject CA Managers and operators. These are not published and are used only for announcements pertaining to the Root CA, or announcements affecting all Subject CAs.

9.5 Intellectual Property Rights

This document contains headings from RFC3647, and the content is structured according to the recommendations of that document.

Section 9 contains text derived from, or copied from, the UK Department of Trade and Industry (DTI) supplementary example agreements from the Lambert Working Group on Intellectual Property, and from the DTI Office of Science

and Technology LINK CBI/AURIL model collaboration agreement. This is all Background IP.

The owner of the Foreground Intellectual Property (IP) in this document is CCLRC. CCLRC grants a non-exclusive indefinite licence to any other Grid or academic CA in the World, to use this IP for related purposes, including to sub-licence to other Grid or academic CAs, provided the source is acknowledged. Such an acknowledgment must acknowledge "the UK e-Science CA run by CCLRC."

9.6 Representations and Warranties

When issuing a certificate to a Subject CA, the Root CA will have evaluated the CP/CPS of the Subject CA, and is satisfied that the Subject CA, when operating according to its CP/CPS, complies with the requirements imposed on it by this document.

9.7 Disclaimers of Warranties

CCLRC makes no representation and gives no warranty, condition or undertaking in relation to the Root CA and its operation.

The Root CA does not audit any Subordinate CA, and makes no assertion that any Subordinate CA is operating according to its own CP/CPS.

9.8 Limitations of Liability

In respect of the information published by the Root CA, including, but not limited to certificates and CRLs, the Root CA shall make best endeavours to ensure the information is timely and accurate. CCLRC shall be under no obligation or liability, and no warranty condition or representation of any kind is made, given or to be implied as to the sufficiency, accuracy or fitness for purpose of such information. The recipient party, whether CA, RP, EE, or anyone else, shall in any case be entirely responsible for the use to which it puts such information.

9.9 Indemnities

Each Subject CA and RP must indemnify the CCLRC and keep the CCLRC indemnified against any and all damages, costs, claims or expenses, which are awarded against, or suffered by the Subject CA or RP or their hosting institution or company, as a result of any act or omission of the RP, Subject CA, or any of the Subject CA's Subordinate CAs.

9.10 Term and Termination

The Root CA shall announce its termination widely, to subject CAs and major RPs, and PMAs. The announcement should be made five years, or the maximal lifetime of any valid Subject CA certificate, whichever is shorter, prior to actual termination. The Root CA shall issue no certificate whose lifetime will exceed the date of termination. The Root CA shall be under obligation to maintain the CRL until its termination.

9.11 Individual notices and communications with participants

A mailing list shall be maintained for announcements pertaining to the Root CA, or announcements affecting all Subject CAs.

9.12 Amendments

The Root CA shall communicate amendments to Subject CAs, and its relevant PMA.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

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

If any part or any provision of this document shall to any extent prove invalid or unenforceable in law, including the laws of the European Union, the remainder of such provision and all other provisions of this document shall remain valid and enforceable to the fullest extent permissible by law, and such provision shall be deemed to be omitted from this document to the extent of such invalidity or unenforceability. The remainder of this document shall continue in full force and effect and the Root CA and Subject CAs and RPs shall negotiate in good faith to replace the invalid or unenforceable provision with a valid, legal and enforceable provision which has an effect as close as possible to the provision or terms being replaced.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.