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

Jens G Jensen

Rutherford Appleton Laboratory

17 July 2002

Contents

Chapter 1

INTRODUCTION

This document describes the rules and procedures used by the e-Science Certification Authority. In the following it is assumed that the subscriber is someone participating in an e-Science programme who wishes to apply for an X.509 digital certificate to identify themselves within the UK e-Science Grid.

1.1 Overview

This document is a draft, structured according to RFC 2527

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)

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 Practice Statement (CPS)	A statement of the practices, which a certification authority employs in issuing certificates.
GridPP Collaboration	UK Particle Physics collaboration funded by PPARC.
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 accompanies a certificate policy identifier in an X.509 certificate.

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 online, which contains lists of issued certificates, CRLs, policy documents, etc.
Subscriber	A person or server to whom a digital certificate is issued. 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	0.7
Document date	17 July 2002
Document OID	1.3.6.1.4.1.11439.1.1.1.1.1

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.

1.3.3   End Entities (Subscribers)

The e-Science CA issues certificates for e-Science projects funded by the UK Research Councils. The CA will issue certificates for both people and servers and services.

1.3.4   Applicability

Certificates issued are of the following types:

- for e-mail signing and encryption (S/MIME)
- for server certification and encryption of communications (SSL/TLS);
- Personal
- Server
- Object Signing

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 is:

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

Phone: +44 1 235 446104
Fax:   +44 1 235 446626
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:

- issue certificates to entitled subscribers based on validated requests from Registration Authorities;

- notify the subscriber of the issuing of the certificate;

- send the certificate to the subscriber by email;

- 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 a Certificate Revocation List (CRL);

- publish the CRL.

2.1.2 RA Obligations

The RA must:

- adhere to Subscriber's Obligations (2.1.3)

- accept certification requests from entitled entities;

- authenticate the identity of the subscriber and keep a log of how each subscriber was authenticated;

- 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);

- check that the subscriber is adequately safeguarding their private key - for a personal key, this means that the key is protected by a pass-phrase of length at least 15 characters; for a server key it means that the key is at least readable only by root;

- check that the information provided in the certificate request is correct and check that the email address provided by the subscriber is correct;

- sign the request;

- inform the CA and request the revocation of the RA's certificate if the RA's private key is compromised or suspected to be compromised.

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];

- take every precaution to prevent any loss, disclosure or unauthorised access to or use of the private key associated with the certificate, including:

- selecting a pass-phrase of at least 15 characters (personal certificates);

- protecting the pass-phrase from others (personal certificates);

- notifying immediately the e-Science CA and any relying parties if the private key is lost or compromised.

2.1.4 Relying Party Obligations

The Relying Party must:

- read the procedures published in this document;

- verify the CRL before validating a certificate;

- use the certificates for the permitted purposes only.

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 when they are updated or at least once a week.

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 a digitally signed request from the subscriber, or the RA which authenticated the subscriber, or if it has itself reasonable proof that the certificate has been compromised. 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, and to request revocation of a certificate if a subscriber's private key has been compromised or a subscriber's eligibility for a certificate has changed.

2.3   Financial Responsibility

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

2.4   Interpretation and Enforcement

2.4.1   Governing Law

Interpretation of this policy is according to UK Law.

2.5   Fees

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

2.6   Publication and Repositories

2.6.1   Publication of CA information

The e-Science CA operates an online repository 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 whenever they are updated or at least every week.

- This CP/CPS will be published whenever it is updated.

2.6.3 Access controls

The online repository 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 runs 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

A self-assessment by CLRC, 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 Compliance Audit per year when requested by a Relying Party and performed by any UK government or academic institution. The entire cost of such an audit must be borne by the requestor.

2.8 Confidentiality and the Data Protection Act

The e-Science CA collects a subscriber's full name and e-mail address. The subscriber's full name, but NOT e-mail address, is included in the issued certificate. No other subscriber's information is collected. 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). The

information kept is generally publicly available from the organisations' web pages.

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. In the case of RA Managers and Operators, personal contact information is also kept confidential.

2.8.2   Types of information not considered confidential

Information included in issued certificates and CRLs is not considered confidential.

2.8.3   Disclosure of certificate revocation/suspension information

No stipulation.

2.8.4   Release to law enforcement officials

If a certificate is used for encryption, the subscriber could become liable to a disclosure notice under the Regulation of Investigatory Powers Act 2000.

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 [Eur00], [Tru], [NCS99], [FBC99], [Gen01] and [Cec01].

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. It 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.
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 by [IAN]

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.

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. Certificates must apply to unique individuals or resources. Subscribers may 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

This is part of the process for appointing an RA. See section 5.3.

3.1.9 Authentication of Individual Identity

Procedures may differ if the subscriber is a person or a server. These are the minimum checks permitted by this Policy; individual RAs may impose more stringent checks.

In either case the subscriber selects which RA is to carry out the authentication process.

Person	The Subscriber goes to the RA Operator bringing acceptable photo ID. Alternatively, if the RA Operator is able to verify the Subscriber's identity by conversation alone, then the Operator may approve the request by calling the subscriber using a telephone number established by independent means (i.e. a site telephone directory).
Server	Requests for server certificates must be approved in the same way as personal certificates or verified by other appropriate means.

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.

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:

  - Digitally 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 email digitally signed with a certificate which has not expired or been revoked.

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].

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 e-Science RA or by the CA itself.

The CA sends the certificate to the subscriber by email. Alternatively, the subscriber can download the certificate using the CA's web interface.

Once a certificate request has been approved by the RA, 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.

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 the UK Research Councils' e-Science program;

- the subscriber's private key is lost or suspected to be compromised;

- the information in the subscriber's certificate is suspected to be 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 certificate whose revocation is requested; or,

- The revocation request is signed by the RA who originally approved the certificate request.

Otherwise the CA will check using the same procedure as for the authentication of the identity of a person.

4.4.4 Revocation request grace period

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

4.4.5 Circumstances for Suspension

No stipulation.

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 after every certificate revocation or at least every week.

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 issuing 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.

4.6   Records Archival

4.6.1   Types of event recorded

The following events are recorded and archived:

- certification requests;

- issued certificates;

- issued CRLs;

- all e-mail messages received by the CA

- all e-mail messages sent by the CA

4.6.2   Retention period for archive

The minimum retention period is 3 years.

4.7   Key Changeover

No stipulation.

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 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's private key is compromised or suspected to be compromised, the RA will inform the CA and request the revocation of the RA's certificate.

4.9 CA Termination

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

- inform the Registration Authorities, Subscribers and cross-certifying CAs;

- make information of its termination widely available;

- stop issuing certificates.

Chapter 5

PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

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

5.2 Procedural Controls

No stipulation.

5.3 Personnel Controls

- The CA manager must be a paid employee of CLRC and shall be appointed in writing by the CLRC 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 CLRC and will be appointed by the CA manager. It is the responsibility of the CA manager to provide the CA operators with a copy of the "e-Science CA Operator's Procedure".

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

- 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. It is the responsibility of the RA Manager to provide the RA operator with a copy of the "e-Science RA Operator's Procedure". RA Operators must have certificates and must adhere also to the Subscribers' Obligations.

5.3.1 Sanctions for unauthorised 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.

Chapter 6

TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

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

6.1.2 Private key delivery to entity

No stipulation.

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 (including 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 e-Science CA private key is the only key that can be used for signing certificates and CRLs.

The certificate KeyUsage field is used in accordance with [HFPS99].

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

Any backup copy of the private key is kept at least as secure as the one used for signing (i.e. encrypted, and on media locked in a safe).

6.2.5 Private key archival

No stipulation.

6.2.6 Private key entry into cryptographic module

The CA private key is kept encrypted, in multiple copies and in different physically secure locations, on removable media.

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.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

No stipulation.

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 pass-phrase of length at least 15 characters.

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;

- machines are protected by a suitably configured firewall.

6.5.2   Computer Security Rating

No stipulation.

6.6   Life-Cycle Technical Controls

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.

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

Basic Constraints	CA:FALSE
Key Usage	Digital Signature, Non Repudiation, Key Encryption, Key Agreement
Subject Key Identifier	hash
Authority Key Identifier	keyid, issuer
Subject Alternative Name (server only)	contact person email (*not* server FQDN)
Issuer Alternative Name	CA email

CRL Distribution Points	[CAC]
Netscape Cert Type	SSL Client, S/MIME
Netscape Comment	"UK e-Science User Certificate"
Netscape CA Revocation URL	[CAC]
Netscape Revocation URL	[CAC]
Netscape Renewal URL	(no stipulation)

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name Forms

Issuer:

/C=UK/O=eScience/OU=CLRC/L=eScience/CN=CA/Email=ca@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 (grid, host, etc) followed by / (e.g. CN=ldap/ldap.rl.ac.uk).
SubjectAltName	RFC822 compliant email address of requestor (server requests only).

7.1.5 Name constraints

See section 4.1.

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.

7.2 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 don't 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 don't 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.

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.

Bibliography

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

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

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

[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.

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

[HFPS99]   R. Housley, W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. http://www.rfc-editor.org/rfc/rfc2459.txt, January 1999.

[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.

Appendix A

Revision History

Version	Date	Changes
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	17 July 2002	final draft