IST Project 20247

INFORMATION SOCIETY TECHNOLOGIES
(IST)
PROGRAMME

EUROGRID

Application Testbed for European GRID Computing

Technical Action T-03-01. / University of Manchester

Specification of EUROGRID Certificate Authority (CA) Policy

Author(s)	Institution(s)
Jon MacLaren	University of Manchester

Classification:

Status:	Internal
Version:	1.4
Reviewed by:	Project Partners
Distribution:	Project Officer
	Project Reviewers
	Project Partners

Table of Contents

1 Introduction

This document contains the certification guidelines (the so-called "policy" or "certification practice statement", CPS) of the certification authority of the EUROGRID project. This certification authority will be used to issue certificates for both the EUROGRID project (IST project 20247), and the closely-related EU-funded GRIP project (IST-2001-32257).

Section 2 lists abbreviations which are used in this document. Section 3 contains the Certificate Practice Statement, detailing procedural aspects of the certification process. Section 4 gives an overview of how the computational aspects of the procedure will be implemented, what software will be required for the client and how it will be provided. Section 5 describes a timetable for the implementation of the policy (identified as EUROGRID Technical Action T-04-10 in the minutes of the EUROGRID Plenary Meeting held in Rome on October 5, 2001). A change history for this document is contained in Section 6.

2 Abbreviations

CA: Certification Authority

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSR: Certificate Signing Request

DN: Distinguished Name (X.500 name)

EG-CA: EUROGRID Certification Authority

EG-RA: EUROGRID Registration Authority

IANA: Internet Assigned Numbers Authority (http://www.iana.org/)

NJS: Network Job Supervisor

PKCS#12: Personal Information Exchange Syntax Standard

PKI: Public-Key Infrastructure

RSA: Rivest, Shamir, Adleman (developers of the RSA algorithm)

SSL: Secure Sockets Layer

WWW: World Wide Web

3 EUROGRID Certification Practice Statement

This section contains the Certification Practice Statement (CPS) to be used by the EUROGRID Certification Authority. The EUROGRID Certification Authority will henceforth be referred to as EG-CA.

3.1 Identity of the EG-CA

Postal address: EUROGRID-CA
C/O John Brooke, Jon MacLaren
Manchester Computing
Kilburn Building
Oxford Road
Manchester M13 9PL
United Kingdom

E-mail address: eurogrid-ca@eurogrid.org

Validity of this document: Until end of EUROGRID project

Version of this document: 1.4

3.2 Scope of the EG-CA

The EG-CA's sphere of responsibility comprises all organisations / institutions participating in the EUROGRID project, and also the GRIP project.

The EG-CA issues the following certificates:

- certificates for users within the EUROGRID (and GRIP_ projects;
- certificates for gateways and network job supervisors (NJSs) of the sites within the EUROGRID (and GRIP) projects.

This policy supports especially the X.509v3 certificate format used in current standard browsers for different applications (SSL and code signing).

3.2.1 Legal significance

A certification by the EG-CA does not entail any legal significance; there is no legal claim to having a certificate issued by the EG-CA. The purpose of a EUROGRID-wide public key infrastructure (PKI) is to facilitate the accessing of resources provided to the EUROGRID (and GRIP) project partners within in the EUROGRID (and GRIP) projects.

The EG-CA staff as well as the staff members of the EUROGRID registration authorities (EG-RAs) do not assume any form of warranty. All tasks are performed by the PKI staff to the best of their knowledge and belief. Moreover, no liability or warranty under the Digital Signature Act will be assumed.

3.2.2 The EUROGRID certification hierarchy

The EUROGRID-PKI consists of the following levels:

- **EG-CA:**
  - The public key of the EG-CA root certificate is self-signed.

    - Each EG-CA staff member will be able to issue certificates signed by the EG-CA root certificate.

- EUROGRID registration authorities (EG-RAs, see Section 3.2.3)
- The **end entities** are composed of the following groups:
    - users (client certificates for SSL)
    - gateways and NJSs of the EUROGRID sites

All subscribers to the infrastructure receive the EG-CA certificate in the course of their own certification and can thus verify the authenticity and validity of all certificates issued by the EG-CA.

The EG-CA does not certify any sub-CAs. Cross certification with other (P)CAs is not planned for the time being.

3.2.3 EUROGRID Registration Authorities (EG-RAs)

The EUROGRID registration authorities (EG-RAs) are trustworthy persons who verify (register) the identity and authenticity of individual end entities on site on behalf of and for the support of the EG-CA, before these end entities are certified by the EG-CA. The EUROGRID (and GRIP) projects nominates such EG-RAs.

A EG-RA may neither generate asymmetric key pairs for end entities nor can it issue certificates itself; a EG-RA can, however, initiate the revocation of certificates.

The certificate signing request (CSR) of the end entity is transmitted by the end entity (or person acting on behalf of the end entity in the case of Gateway and NJS certificates) to the EG-CA by e-mail. The EG-CA records all such CSRs. The EG-RA responsible for the site where the end entity is located will then be asked to verify the identity of the end entity (or that the end entity is entitled to request certificates on behalf of a Gateway or NJS).

The EG-RA verifies the identity of the end entity in a suitable manner (see Section 0). The EG-RA confirms the verification performed by telephone conversation with the EG-CA, or by an e-mail sent to the EG-CA.

The new certificate issued by the EG-CA is transmitted directly to the end entity. In the case of Gateway and NJS certificates, the certificate will be sent to the person requesting the Gateway or NJS certificate. The returned certificates will be recorded by the EG-CA.

The EUROGRID (and GRIP) projects may nominate any number of persons as EG-RAs. Such persons must present themselves at a EUROGRID (or GRIP) Plenary or Review Meeting, where their identity will be authenticated. The identity of these persons will be recorded in the minutes of the EUROGRID (or GRIP) meeting.

3.3 Security of the EG-CA equipment

Due to the participation in a PKI, as well as there being specific requirements with respect to the security of the hardware and software used by the EG-CA, there are also requirements for all subscribers regarding the safe and reliable handling of cryptographic keys. The

requirements for the EG-CA are naturally higher since the misuse of a EG-CA key would withdraw trustworthiness from all subordinate certificates.

3.3.1 Security requirements for the EG-CA

The following demands are made on the EG-CA:

- All certificates are *exclusively* generated *off line* on a dedicated certification computer which at no time has a network connection. Moreover, this computer is physically immobilised and locked to prevent the theft of the private part of the EG-CA certificate.
- Any data exchange with networked computers will be transferred using floppy disks.
- Information (e.g. the certificates generated) will be made available to the project partners.
- The secret key of the EG-CA for the generation of digital signatures is to be exclusively generated and used by the EG-CA staff on the dedicated certification computer. No copy of this key will be made on any other machine or storage device. If, for some reason, the private key is lost, a message will be sent to all subscribers, i.e. the EUROGRID partners, declaring all certificates signed with this key to be invalid. A new key will be generated; new certificates must then be requested and issued.
- Access to the off line machine is protected by nontrivial passwords (minimum length: 8 characters) which are only known to the EG-CA staff and must never be stored as plain text or sent through unprotected network connections.
- Asymmetric key pairs of the EG-CA for the generation of signatures have a minimum length of 2048 bits RSA (or a comparable level).
- All data must be treated confidentially by the EG-CA; all legal data protection regulations in force must be complied with.

3.3.2 Security requirements for EG-RAs

The following demands are made on the EG-RAs appointed by the EUROGRID (and GRIP) projects:

- All data must be treated confidentially by the EG-RAs; all legal data protection regulations in force must be complied with.

3.3.3 Security requirements for end entities

The following demands are made on all end entities of the EG-CA, or their human representative in the case of Gateway and NJS end entities:

- All asymmetric key pairs for end entities must have a minimum length of 1024 bits RSA (or a comparable level).
- The end entity's secret key (see Section 3.2.2) must be adequately protected against misuse by unauthorized persons and may not be disclosed; each end user is himself responsible for this.

- Access to an end entity's secret key should be protected by setting a nontrivial password (minimum length: 6 characters).

- This password may not be disclosed to other persons.

Security requirements for users (SSL, code signing)

Users in terms of this policy are individual persons forming a subset of the end entities.

- The user must protect access to his secret key by setting a nontrivial password.

- This password must never be filed as plain text (i.e. stored on the disk) or sent through unprotected network connections.

- The directory or files in which the cryptographic keys are stored by the application must be protected by the user against unauthorized misuse as far as possible. This can be achieved, for example, by setting specific rights of access provided that this is supported by the operating system used.

Security requirements for the gateways and NJSs of the EUROGRID sites

- The directory or files in which the cryptographic keys are stored by the application must be protected by the user against unauthorized misuse as far as possible. This can be achieved, for example, by setting specific rights of access provided that this is supported by the operating system used.

- If the password is filed as plain text, e.g. for the purposes of automatic starting of the Gateway or NJS, the directory or files in which the password is stored must be protected by the user against unauthorized misuse as far as possible. As stated above, this can be achieved by setting specific rights of access provided that this is supported by the operating system used.

3.4 Certification rules

This section describes technical and organizational guidelines and procedures to be observed prior to the certification of end entities.

End entities are given distinguished names whose correct choice is of particular significance. The choice of these names is described in Section 3.7.

In order to identify illegal certificate signing requests, the EG-CA will convince itself of the identity of the key holder requesting certification in a suitable manner by technical and organizational measures prior to certification.

The registration process is only possible by *personal contact* with one of the EG-RAs prior to certification. Responsibility lies with that EG-RA. EG-CA staff members may also simultaneously exercise the function of a EG-RA, but must then abide by the rules for EG-RAs.

Under no circumstances will certificates be processed *automatically*, and they are exclusively granted under the following conditions:

- The public key to be certified has the minimum length defined in Section 3.3.3.

- The registering authority (i.e. the EG-CA or a EG-RA) has duly convinced itself of the key holder's identity.

The newly issued certificate is transmitted to the certificate holder immediately after certification by e-mail. The certificate holder is urged to immediately verify the correctness of his own certificate and of the higher-level EG-CA certificates.

Each certificate contains a serial number assigned by the EG-CA, and the EG-CA ensures in the certification process that no serial number has been assigned more than once.

For the time being, certificates are not automatically extended by the EG-CA; applications for re-certification must be filed, where necessary.

3.4.1 Certificate extensions

X.509v3 certificates are characterized by the fact that each certificate may contain arbitrary extensions (certificate extensions). Moreover, each extension can be flagged as particularly significant by setting a particular bit (critical flag).

Certificate extensions are included in the certificate by the U-CA during certification. Although extensions can be proposed in the CSR, these will always be ignored.

The EG-CA makes known all extensions it has supported. In particular, the EG-CA can limit the application of an issued certificate to certain functions (e.g. the signing of objects such as Java applets) by such extensions. The EG-CA will only generate certificates according to X.509v3, and will only support widely used standard extensions (cf. X.509v3, PKIX, Netscape).

The Leibniz Computer Centre of the Bavarian Academy of Sciences (LRZ) has been assigned a private enterprise number ("1.3.6.1.4.1.7650" by the IANA, the Internet Assigned Numbers Authority. The LRZ assigns the object identifier (OID) "1.3.6.1.4.1.7650.1" to the CA of the UNICORE Plus project. By permission, this OID will also be used by the EG-CA. The EG-CA thus introduces a certificate extension in conformity with X.509v3. The certificate extension is called "unicoreKeyUsage" and corresponds to OID "1.3.6.1.4.1.7650.1". The certificate extension can assume the values “'unicoreClient'", '"unicoreGateway"', "unicoreNJS'" and '"unicoreApplet"'.

The following extensions will be added by the EG-CA:

- All User certificates will all be marked with the unicoreKeyUsage extension set to unicoreClient. Also, the keyUsage extension will be set to digitalSignature, keyEncipherment, keyAgreement to facilitate codesigning.

- All NJS and Gateway certificates will be marked with the unicoreKeyUsage extension set to unicoreNJS and unicoreGateway respectively, to avoid each EUROGRID site having to manually authorise all other NJS or Gateway certificates. Also, the keyUsage extension will be set to digitalSignature, keyEncipherment.

Important Note

Until November 2002, the “nsCertType” extension was being used, with NJS and Gateway certificates being set to “SSL server” only. This was incorrect, as NJSs need to act as clients when consigning sub-AJOs. Java 1.4.0 and 1.3.x allowed NJS certificates to still be used as

SSL clients, as they treated the nsCertType extension as non-critical. This changed in Java 1.4.1. On November 12th 2002, the EG-CA changed the certificate extensions used. The (deprecated) nsCertType extension is no longer used. Instead, combinations of basicConstraints, keyUsage and extendedKeyUsage are used. The precise combinations of these extensions are detailed in the below. This change means that NJS certificates issued before this time (hexadecimal serial numbers 0x800055 and earlier) are not suitable for use with Java 1.4.1. All later certificates (0x800056 and later) use the new extensions, and are compatible with Java 1.3.x and Java 1.4.x.

- **basicConstraints** is set to CA:FALSE for all end entities (this is as before)
- **keyUsage** is set to keyAgreement, dataEncipherment, keyEncipherment, and digitalSignature for all end entities.
- **extendedKeyUsage** is set to serverAuth and clientAuth for all entities, with codeSigning, emailProtection and timeStamping also being provided in User certificates.
- **nsCertType** (which is deprecated) is no longer used.

3.4.2 Rules for the certification of end entities

End entities wishing to be certified first generate a personal asymmetric key pair and subsequently transmit the CSR to the EG-CA by e-mail.

The end entities must *personally* introduce themselves to, or already be known by, one of the EG-RAs. Only in this way will it be possible to verify the end entities' identity and correctly allocate the information contained in the certificate to the end entities.

Unless they are revoked earlier, all end entity certificates will be valid until the 31st of January 2004, i.e. until just after the end of the EUROGRID project.

Additional rules for the certification of the Gateways and NJSs of the EUROGRID sites

In addition to the above-described certification rules for end entities, specific guidelines are valid for the certification of the gateways and NJSs of the EUROGRID sites which are not allocated to an individual but to a computer (name).

An administrator of the EUROGRID site whose gateways and NJSs are to be certified transmits the CRS to the EG-CA. The EG-CA will then ask the EG-RA responsible for the site to verify the following:

- affiliation of the server to a specific organization
- identity of the organization
- identity of the server administrator

The CSR is transmitted for the time being via e-mail.

3.5 Management of certificates

All subscribers to the EUROGRID-PKI implicitly agree to the publication of their certificate.

The EG-CA will publish all issued certificates on the EUROGRID project website (http://www.eurogrid.org). These include the EG-CA root certificate, and all Gateway and NJS certificates, as well as user certificates. Certificates will be posted within one week of being issued. A copy of the current CRL (see Section 3.6) will also be posted to the EUROGRID website within this time.

3.6 Revocation of certificates

The EG-CA can revoke certificates issued by it at any time prior to the expiry of the period of validity without explicitly specifying any reasons. Causes for the revocation of a certificate may be, for example, the discovery of improper actions by a EG-CA staff member or failure to comply with individual guidelines of this policy. Other reasons may be a EG-CA staff member leaving an institution or a change of name.

Each certificate holder can request the EG-CA or that EG-RA which has certified him to revoke or initiate the revocation of a certificate issued for him without giving reasons. The EG-CA will comply with this request within a reasonable period of time as soon as it has convinced itself by taking suitable steps that the request has been made or authorized by the certificate holder himself.

If a subscriber's own secret key is known to have been misused or compromised, each such subscriber should immediately notify the EG-CA or the relevant EG-RA and initiate the revocation of his own certificate.

Certificates can only be revoked by the EG-CA. However, the EG-RA responsible for verifying the identity of a certificate holder can initiate a revocation of that certificate without giving reasons.

All revoked certificates are published by the EG-CA in a CRL made available to all subscribers. This CRL contains the date of CRL issuance (e.g. in the form of a time stamp) and is digitally signed by the EG-CA. Revoked certificates remain in the CRL until the original validity period has been exceeded. Those certificates whose publication has been objected to during certification are also published in a CRL.

Certificates once revoked cannot be renewed or extended. However, each subscriber basically has the possibility of applying for a new certificate.

Immediately after starting its own operation, the EG-CA will issue a new (empty) CRL. Subsequently, new CRLs will be issued at regular intervals (e.g. monthly), even if no further certificates have been revoked by the EG-CA in the meantime. Old CRLs will be archived to enable verification of the validity of certificates even at a later date.

For making CRLs publicly available the EG-CA establishes information services (directories) whose task is to distribute certificates and CRLs (see Section 3.5). Since many software products at present only insufficiently support the processing of CRLs, the EG-CA will inform its certificate holders accordingly and, if possible, implement solutions of its own for CRL distribution.

3.7 Rules for naming

All certificate holders are assigned a distinguished name (DN) to be used upon issuance of a certificate for a subscriber as his subject name. A DN contains a sequence of uniquely identifying name attributes by which all the subscribers in a hierarchy can be referenced; no umlauts, unusual special characters etc. will be used within this DN for reasons of interoperability.

Prior to certification, the correctness and uniqueness of the specified DN is verified by the EG-CA; no name is assigned more than once.

The DN of each user follows the scheme below:

CN = "<*complete name*>",
EMAIL = "<*e-mail address*>",
O = "<*organisation*>",
[OU = "<*organisational unit*>",]
[L = "<*city or locality*>",]
[ST = "<*state/province*>",]
C = "<*country*>"

Deviations from this scheme are only possible after prior agreement with the EG-CA.

3.7.1 Choice of a name for EG-CAs and end entities

The choice of unique end entity DNs is primarily governed by the EG-CA guidelines. EG-RAs are subject to the same rules for naming as users.

The attribute "CN=" is obligatory for all end entities and occurs precisely once. It contains the complete name of the user.

A valid e-mail address is adopted in the DN via the attribute '"EMAIL="'. Optionally, further attributes such as "OU=" ("organizational unit"), "L=" ("city/locality") and "ST" ("state/province") can be included in the DN.

If a name occurs several times within one organization, the EG-CA will choose unique DNs by suitable name additions. The EG-CA is furthermore responsible for checking the affiliation of the user to the institution concerned and for ensuring that all certified users have different DNs. This is done with the aid of a EG-RA.

Additional rules for the gateways and NJSs of the EUROGRID sites

Certificates for the gateways and NJSs must contain a distinguished name in the "CN=" attribute. This attribute must not contain wildcards nor any numerical IP addresses.

The optional attribute "EMAIL=" must contain a valid e-mail address (e.g. the address of the server administrator).

3.8 Miscellaneous

This document was drawn up under the EUROGRID project at Manchester Computing, the University of Manchester. It was based upon V0.9 of the UNICORE-CA Policy Document, by Dr Ernst Bötsch.

No liability is assumed for the correctness, completeness or applicability of the information contained and the measures proposed. Furthermore, no liability can be assumed for possible damage arising from making use of the EG-CA services.

The EG-CA reserves the right not to fulfil certificate signing requests. Furthermore, no guarantee can be assumed for the availability of the EG-CA services. On account of the status as a research project, there is at present no possibility of offering the EG-CA services on a 7-day/24-hour basis.

3.8.1 Documentation and data protection

All activities within the framework of this policy will be documented as far as technically feasible. The EG-CA, all EG-RAs and all EUROGRID staff members having access to data must treat the data arising in certification as confidential and comply with the respective data protection guidelines.

All subscribers to EUROGRID-PKI (i.e. end entities, EG-CA staff and EG-RAs) agree to the storage and processing of their data by the EG-CA.

Declaration by the EG-CA staff

The agreement of EG-CA to abide by this Policy document will be recorded in the minutes of a EUROGRID Plenary or Review meeting.

Declaration by the EG-RAs

The agreement of EG-RAs to abide by this Policy document will be recorded in the minutes of a EUROGRID Plenary or Review meeting.

Declaration by the end entities

All end entities of the EUROGRID-PKI implicitly agree to this Policy document when they submit a request for certification to the EG-CA.

Fees

The EG-CA will not impose fees for its services.

4 Software implementation of the EUROGRID CA Policy

Members of the EUROGRID (and GRIP) projects will be provided with tools to:

- enable them to request certificates;
- generate PKCS#12 files using their private key, and their EG-CA signed certificate.

The tools will be provided in the form of UNIX Korn-shell scripts. The scripts will use OpenSSL 0.9.6. Therefore, to request certificates, end entities must have access to a UNIX machine with OpenSSL 0.9.6 (or a more recent version), which has had the EG-CA tool scripts installed on it. OpenSSL can be freely obtained from the OpenSSL WWW page, http://www.openssl.org/.

Due to a bug in the Sun JSSE libraries, which the EUROGRID client software uses, users will also require access to a Netscape WWW browser. Netscape can be freely obtained from the Netscape WWW page, http://www.netscape.com/.

The scripts will be provided via the EUROGRID Project shared document server, and will be bundled with a copy of the EG-CA public certificate.

In the future, it may be possible to use the WWW-page based certification software that is used in the UNICORE Plus project. At time of writing, it is not known if this will be possible.

5 Timetable for the Implementation of the CA Policy

The policy is to be implemented by University of Manchester as Technical Action T-04-10 ("UoM implements CA scheme"), as recorded in the minutes of the EUROGRID Plenary Meeting held in Rome on October 5, 2001.

- EG-RAs were initially identified at the EUROGRID Project Review meeting on the 11th of December 2001. New RAs have been added since then, and the current list is as follows:
  - Bergen: Csaba Anderlik
  - ICM: Piotr Bala
  - T-Systems: Michael Sattler
  - Pallas: Klaus-Dieter Oertel
  - FECIT: David Snelling
  - EADS: Gillaume Alleon
  - FZ-Jülich: Daniel Mallmann
  - CSCS: Nello Nellari
  - IDRIS: Victor Alessandrini
  - DWD: Geerd-R. Hoffmann
  - UoM: Jon MacLaren
  - Southampton: Denis Nicole
- Default base DN for EUROGRID partner sites were decided and are as follows:
  - Bergen: OU=Parallab, O=University of Bergen, L=Bergen, C=NO
  - ICM: OU=ICM, O=Warsaw University, C=PL
  - T-Systems: OU=T-Systems UK, O=T-Systems, L=Milton Keynes, C=GB
  - Pallas: O=Pallas, L=Bruehl, C=DE
  - FECIT: OU=FECIT, O=Fujitsu, L=Hayes, ST=Middlesex, C=GB
  - EADS: OU=GIE EADS CCR, O=EADS, L=Blagnac, C=FR
  - FZ-Jülich: OU=ZAM, O=Forschungszentrum Juelich, L=Juelich, ST=NRW, C=DE
  - CSCS: O=CSCS, L=Manno, C=CH
  - IDRIS: OU=CNRS, O=IDRIS, L=Orsay, C=FR
  - DWD: O=DWD, L=Offenbach, C=DE
  - UoM: OU=Manchester Computing, O=University of Manchester, L=Manchester, C=GB
- Requests for revisions to this document will be considered until the end of the January 2002.
- Default base DNs will be incorporated into the EG-CA tool scripts, which will then deployed (uploaded to the EUROGRID Project shared document server) at the end of January 2002.

- CSRs will then be accepted, based on the CA Policy contained in the revision of this document which is current at the beginning of the February 2002.

This timetable may be subject to alterations, which will be reflected in subsequent versions of this document.

6 Change History

This section briefly documents the modifications of this policy in the transition to the respective next version and is not an integral part of the policy:

1.0 This version is to be provided to the partners for review.

1.1 The following changes were made:

- Certificate extensions will be used to provide codesigner facilities, as well as NJS and Gateway identification.
- Certificates will be issued to be valid until 31st January 2004.
- The list of default DN parts was added.
- The initial list of RAs was added.
- The timetable for script provision and issuing certificates was put back by 1 month.

1.2 The following change was made:

- In Section 3.4.2, the previous version incorrectly stated that end entities must transmit their CSRs to the responsible EG-RA, rather than the EG-CA, contradicting Section 3.2.3 – this was ammended.

1.3 The following changes were made:

- The scope of the EG-CA has been extended to include the GRIP project – this has incurred changes to various sections.
- Certificates and CRLs will not be uploaded to the BSCW any more – they will only be published on the EUROGRID website.

1.4 The following changes were made:

- Denis Nicole added for EG-RA at Southampton
- The certificate extensions used have changed as of November 12th 2002 (hexadecimal serial numbers 0x800056) and above. See “Important Note” in Section 3.4.1 (page 6).