
# Certification Authority
# AUSTRIANGRID CA

## Certificate Policy and
## Certification Practice Statement

VERSION 1.2.0

Document OID: 1.3.6.1.4.1.21356.1.1.1.2.0

May 2, 2007

# Contents

# 1 INTRODUCTION

This document is based on the framework outlined by the IETF RFC 3647 [1] which obsoletes RFC 2527 [2], and structured as proposed therein.
The Public Key Infrastructure (PKI) used for the implementation of the policy described by this CP/CPS document is derived from the requirements and recommendations of RFC 3289 [3] which obsoletes RFC 2459 [4].

## 1.1 Overview

The AUSTRIAN GRID[5] is an initiative funded by the Austrian Federal Ministry for Education, Science and Culture to set up a Grid infrastructure and leverage Grid computing.
This document describes the set of rules and operational practices shall be used by AUSTRIANGRID CA, the Certification Authority (CA) for the AUSTRIAN GRID for issuing certificates. This and any subsequent CP/CPS document can be found on its web site `http://www.austriangridca.at`.
The AUSTRIANGRID CA issues certificates only to entities associated with members of the AUSTRIAN GRID Consortium and to members of the e-Science community in Austria for use in academic or non-academic Grid and e-Science related research and development activities.

## 1.2 Document name and identification

| | |
|---|---|
| Title: | AUSTRIANGRID CA Certificate Policy (CP) and Certification Practice Statement (CPS) |
| Version: | 1.2.0 |
| Date: | May 2, 2007 |
| Expiration: | This document is valid until further notice. |
| OID assigned: | 1.3.6.1.4.1.21356.1.1.1.2.0 |
| OID structure[10]: | |
| IANA: | 1.3.6.1.4.1<br>iso(1).org(3).dod(6).internet(1).private(4).enterprise(1) |
| AUSTRIAN GRID: | 21356 |
| AUSTRIANGRID CA: | 1 |
| This CP/CPS document: | 1 |
| Version of this CP/CPS: | 1.2.0 |

## 1.3 PKI participants

### 1.3.1 Certification authorities

The AUSTRIANGRID CA doesn't issue certificates to subordinate Certification Authorities.

### 1.3.2 Registration authorities

The AUSTRIANGRID CA also performs the role of a Registration Authority (RA). Each partner of the AUSTRIAN GRID Consortium may appoint an individual who will act as RA for its own members and servers. Further RAs that provide service to any eligible entity may be installed at academic institutions all over Austria. The list of RAs for the AUSTRIAN GRID is available from the AUSTRIANGRID CA website `http://www.austriangridca.at`

### 1.3.3 Subscribers

The AUSTRIANGRID CA may issue certificates for

- **natural persons** associated with
- **automated systems** operated by
- **services or applications** offered by

institutions, groups or individuals associated with members of the AUSTRIAN GRID Consortium or with the e-Science community in Austria for use in Grid or e-Science related research and development activities.

### 1.3.4 Relying parties

Relying parties may be:

- natural persons receiving signed e-mails, or accessing hosts or services
- hosts to which certificate owners login or send processes or jobs
- services called by owners of a certificate

associated with Grid or e-Science related research and development activities.

### 1.3.5 Other participants

No stipulation

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

CA certificates and their associated private keys may only be used to issue certificates and for checking certificates that claim to be issued by the AUSTRIANGRID CA.
RA certificates and their associated private keys may only be used by the RA agent for RA related activities, not for other activities of that natural person; these must be undertaken using an end-entity certificate and associated private key.

The end-entity certificate may be used for any application that is suitable for X.509 certificates, in particular:

- authentication of users, hosts and services
- authentication and encryption of communications
- authentication of signed e-mails
- authentication of signed objects

They may only be used or accepted for actions related to Grid or e-Science research and development and authorised by the certificate keys.

### 1.4.2 Prohibited certificate uses

The certificates issued by AUSTRIANGRID CA must not be used for commercial or financial transactions.
They must not be used for actions which require "qualified certificates" according to the Austrian Signature Act (Signaturgesetz - SigG) [6] and Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [7] because the AUSTRIANGRID CA doesn't comply with §7(1)6 of the SigG and Annex II, point (h) of Directive 1999/93/EC concerning the financial resources for covering liabilities for damages (see also subsection 9.8).
They must not be used for purposes that violate Austrian law or the law of the country in which the target entity (e.g. application or host to use, addressee of an e-mail) is located.

## 1.5 Policy administration

### 1.5.1 Organisation administering the document

The AUSTRIANGRID CA is responsible for the registration, maintenance, and interpretation of this CP/CPS. It is reachable at:
VCPC
Institute of Scientific Computing
University of Vienna
Nordbergstrasse 15/C/3
A-1090 Vienna
Austria, Europe
Home page: `http://www.austriangridca.at`

### 1.5.2 Contact person

Willy Weisz (manager of the AUSTRIANGRID CA)
VCPC

Institute of Scientific Computing
University of Vienna
Nordbergstrasse 15/C/3
A-1090 Vienna
Austria, Europe
Phone: +43 (0)1 4277 38824
Fax: +43 (0)1 4277 9388
e-mail: weisz@vcpc.univie.ac.at

For contacting anyone in charge of AUSTRIANGRID CA activities messages should be sent to:
e-mail: ca@austriangrid.at

### 1.5.3 Person determining CPS suitability for the policy

The manager of the AUSTRIANGRID CA (see 1.5.2) is responsible for determining the CPS suitability for the policy.

### 1.5.4 CPS approval procedures

CP/CPS changes shall be submitted to the AUSTRIAN GRID Policy Administration Authority (PMA) for approval.
The approved document shall then be submitted to EUGridPMA for acceptance in European e-Science projects.

## 1.6 Definitions and acronyms

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [8].

| | |
|---|---|
| PMA | Policy Administration Authority, established by the AUSTRIAN GRID Project Co-ordination Committee, consisting of at least 3 persons (including the AUSTRIANGRID CA manager), responsible for defining the operation of the AUSTRIAN GRID PKI according to this CP/CPS. |
| CSR | Certificate Signing Request containing the public key of a key pair and formatted according to the syntax of PKCS #10 [9]. |

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

The online repository of information from the AUSTRIANGRID CA is accessible at the URI `http://www.austriangridca.at`.

## 2.2 Publication of certification information

The AUSTRIANGRID CA shall maintain a public World Wide Web server with unlimited access. The information made available on this site shall include:

- the AUSTRIANGRID CA root certificate, and all previous ones necessary to check still valid certificates,
- the list of revoked AUSTRIANGRID CA certificates (CRL),
- all valid AUSTRIANGRID CA certificates,
- the CP/CPS document in effect as well as all previous versions based on which certificates are still valid, and
- if available, documentation to support subscribers who want to use the services of the AUSTRIANGRID CA.

## 2.3 Time or frequency of publication

All information published shall be up-to-date.
The certificates shall be made available as soon as they are accepted, checked and confirmed by the subscriber (see 4.4.1).
The certificate revocation list (CRL) shall have a lifetime of at most 30 days. The AUSTRIANGRID CA must issue a new CRL at least 7 days before expiration or immediately after having processed a revocation, whichever comes first. A new CRL must be published immediately after its issuance.

## 2.4 Access controls on repositories

The information on the AUSTRIANGRID CA web site are accessible without any restriction. If misuse of the data is evident, access controls may be enacted in order to protect the owners of certificates.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

The names used in the certificate subject name and issuer name fields shall be in the form of full X.501 distinguished names (DN).
The subject alternative name entry in a certificate for a natural person shall be in the form of e-mail adresses according to RFC 822 ([11]).

### 3.1.2 Need for names to be meaningful

Names used in the different entries of a certificate issued by the AUSTRIANGRID CA must allow the identification of the subject and of its affiliation.
e-mail addresses that appear in the alternative name entries must be real addresses to which messages can be sent in order to reach the subject .

### 3.1.3 Anonymity or pseudonymity of subscribers

No natural-person certificates shall be issued to roles or functions, only to named and identified persons.

### 3.1.4 Rules for interpreting various name forms

The CN component of the subject name in a certificate for a natural personal must contain the first and the family name as it appears in the authentication document proving the name of the subscriber.
The CN entry for a host shall be the fully qualified domain name (FQDN) that can be universally used to access that host.
The CN entry for a service shall be the name of the application followed by a slash (“/”) followed by the FQDN of the host on which the application is executed.

### 3.1.5 Uniqueness of names

The Distinguished Name must be unique for each entity that owns a certificate issued by the AUSTRIANGRID CA. If the name presented by the requesting party is not unique, the CA shall ask the requesting party to resubmit the request with some variation in the Common Name (CN) entry to ensure uniqueness. In this policy two names for a natural person or a service/application are considered identical if they differ only in case or punctuation or whitespace; in other words case, punctuation or whitespace must not be used to make the difference.

### 3.1.6 Recognition, authentication and role of trademarks

No stipulation

## 3.2 Initial identity validation

### 3.2.1 Method to prove possession of private key

The possession of the private key by the requestor is considered proven when the signature of the certificate signing request (CSR) is verified using the public key present in the request.

### 3.2.2 Authentication of organisation identity

The RA shall verify that the requesting party's organisation or a unit of an organisation is entitled (see 1.3.3) to get a certificate from the AUSTRIANGRID CA and that it consents to the request.
The first time an organisation/unit wants to get a certificate for a natural person, a server or a service, or wants to install an RA, it has to announce this officially to the appropriate RA or the AUSTRIANGRID CA. The RA has to ascertain that the organisation or organisational unit exists and is entitled to request an AUSTRIAN GRID certificate. It must also get competent information on who is entitled to sign on behalf of the institution.

### 3.2.3 Authentication of individual identity

In order to enable the RA to authenticate the individual's identity the latter must meet in person with the RA and present an officially recognised document proving the requesting party's identity (e.g. a passport).
The RA shall send via a secure communication channel or in a signed e-mail to the AUSTRIANGRID CA (a) an electronic copy of the pages of the requesting party's identification document containing the personal data items that are part of the certification request submission and a photograph of the document owner, and (b) the certification request. The information will be stored in a database at the CA site and be considered as private and confidential (see 9.4).
If a requesting party fails to meet the authentication requirements within 9 days after the request has been received by the RA, the request is void, and a new one has to be submitted.

### 3.2.4 Non-verified subscriber information

No stipulation

### 3.2.5 Validation of authority

In a statement, preferably written and signed by an individual authorised by the organisation to sign on behalf the organisation or the unit, - the RA has to ascertain the authorisation - the organisation shall nominate one or more representatives who are entitled to request server or service/application certificates and answer all questions related to natural-person certificate requests.

These natural persons shall be the first in their organisation/unit to request individual certificates according to the provisions outlined in 3.2.3. The signatures of these individuals with the private key associated with the certified public key shall be sufficient for all future information exchanges with or requests from that organisation/unit.
When the organisation/unit rescinds the individual's authorisation it has to inform the RA and the AUSTRIANGRID CA in the same way as it has made the authorisation known.

#### 3.2.6 Criteria for Interoperability

No stipulation

### 3.3 Identification and authentication for re-key requests

#### 3.3.1 Identification and authentication for routine re-key

Rekey before the certificate expires can be done by sending a rekey request based on a new public key in an e-mail signed with the old private key to the appropriate RA. After expiration of the certificate no rekey is possible; a new application for initial registration must be made instead.

#### 3.3.2 Identification and authentication for re-key after revocation

After revocation of a key, no re-key is possible. A new application for initial registration must be made.

### 3.4 Identification and authentication for revocation request

Unless the revocation request originates from the AUSTRIANGRID CA because it has independently verified that a key compromise has occurred, the revocation request has to be verified and the requesting party has to be authenticated as described for the authentication of the certification request.
Such a request coming from an RA must be made in a signed e-mail sent to the CA. Before revoking a certificate the AUSTRIANGRID CA has to authenticate the source of the request as it did for the request for certification. Such a revocation request must be made by:

- the owner of the certificate in an e-mail signed with the private key associated with the (still not expired) certificate,
- on behalf of the owner who has lost his/her private key in an e-mail signed by an authorised person of the organisation/unit that consented to the certificate,
- on behalf of the organisation/unit that consented to the certificate in an e-mail signed by an authorised person (see 3.2.2), or

- the appropriate RA that has knowledge of a key compromise.

In case of emergency if no such e-mail can be sent, the revocation can be initiated via oral communication with the appropriate RA or the AUSTRIANGRID CA. The RA or the AUSTRIANGRID CA have to use their best effort to authenticate the request.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 Certificate application

### 4.1.1 Who can submit a certificate application

The AUSTRIANGRID CA issues certificates to eligible organisations, i.e. members of the AUSTRIAN GRID consortium or organisations co-opted into the AUSTRIAN GRID by the executive of the AUSTRIAN GRID consortium, for:

- natural persons for which they take full responsibility,
- hosts administered by the requesting organisation, and
- services provided on a host that is administered by an eligible organisation.

### 4.1.2 Enrollment process and responsibilities

The requesting party generates the key pair with a size of at least 1024 bit on their system through the form provided at the AUSTRIANGRID CA web site. After the form has been completed the encrypted private key will be stored on the system where the browser runs in a file only accessible to the requestor (if the operating system allows such a restriction), and the CSR will be sent to the appropriate RA and the AUSTRIANGRID CA.
If using the browser for this purpose is not appropriate (e.g. when the key pair is generated by a secure hardware device) the CSR in PKCS #10 format [9] must be generated using appropriate software (e.g. OpenSSL) and sent to the appropriate RA and the AUSTRIANGRID CA; in this case the requestor has to contact the RA beforehand to get the correct DN to be included in the request.
Natural persons submit their application which must be acknowledged by the sponsoring organisation that appears in the certificate.
For host or service certificates the CSR or the e-mail containing the CSR must also be signed by the nominated representative (see 3.2.5) of the organisation or unit with his/her personal private key.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

After an RA receives a certification request it must check the electronic signature of the CSR. In the case of a server/service request it must also check that the message is signed by a representative (see 3.2.5) of the organisation or unit responsible for the host.

### 4.2.2 Approval or rejection of certificate applications

Upon successful authentication an electronic copy of the requesting party's identification document and the certification request shall be sent signed by the RA to the AUSTRIANGRID CA. Alternatively, a secure transmission to the AUSTRIANGRID CA may be used, if it is at least as secure as a signed e-mail.
If the authentication information proves to be inaccurate or if a requesting party fails to meet the authentication requirements within 9 days after the request has been received by the RA, the request shall be rejected. If the requesting party insists on getting a certificate it has to initiate a new request.

### 4.2.3 Time to process certificate applications

The turn-around time from request to issuance is typically up to 11 days, depending mostly on the authentication process.

## 4.3 Certificate Issuance

### 4.3.1 CA actions during certificate issuance

The CSR shall be transfered to the computer which holds the private key of AUSTRIANGRID CA and which is not connected to any network. On this system the certificate is created and signed. The signed certificate shall then be transfered back to the online CA server.

### 4.3.2 Notification to subscriber by the CA of issuance of certificate

The AUSTRIANGRID CA shall then send the certificate to the requesting party in an e-mail signed by the CA agent's certified private key. It shall also send an acknowledgement of the issuance to the appropriate RA.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct constituting certificate acceptance

Upon receipt of the e-mail with the certificate the requesting party shall check the signature of the e-mail. He/she shall then sign an arbitrary file with his/her private key and check the signature with the returned certificate and/or encrypt a file using the public key of the certificate and decrypting it with the private key. The requesting party shall notify the AUSTRIANGRID CA of the result of the check for useability of the certificate in conjunction with the private key in its possession. If it was successful and there are no objections to other aspects of the certificate, the subscriber must inform the AUSTRIANGRID CA and the appropriate RA that he/she accepts the certificate. In case of rejection of the certificate, the requesting party must inform the CA and the RA of the rejection and explain the reasons.

Certificates whose acceptance have not been confirmed within a month shall be revoked by the AUSTRIANGRID CA.

#### 4.4.2 Publication of the certificate by the CA

Upon receipt of a certificate acceptance the AUSTRIANGRID CA shall make available the certificate on its repository (see 2.1).

#### 4.4.3 Notification of certificate issuance by the CA to other entities

The AUSTRIANGRID CA shall inform the RA of the acceptance and send it a copy of the certificate.

### 4.5 Key pair and certificate usage

#### 4.5.1 Subscriber private key and certificate usage

Certificates issued by the AUSTRIANGRID CA and their associated private keys must only be used according to the permissions and prohibition stated in section 1.4. They must only be used according to the key usage fields of the certificate. When a certificate is revoked or has expired the associated private key shall not be used anymore.

#### 4.5.2 Relying party public key and certificate usage

A relying party must, upon being presented with a certificate issued by the AUSTRIANGRID CA, check

- its validity by
  - checking that it trusts the CA that issued the certificate,
  - checking that the certificate hasn't expired
  - consulting the AUSTRIANGRID CA CRL in effect at the time of use of the certificate or querying the certificate's validity using the OCSP facility, after its planned installation.
- the appropriate usage as outlined in the CP pointed to by the certificate and in the usage keys included in the certificate.

### 4.6 Certificate renewal

#### 4.6.1 Circumstance for certificate renewal

Due to the danger of exposure of keys that are used for too long, in general AUSTRIANGRID CA certificates are not renewed for the same key pair when they are about to expire. Only in case of extreme necessity, and when the protection of

the private key can be ascertained by the appropriate RA, shall the CA accept and process a renewal request.

### 4.6.2 Who may request renewal

The owner of a certificate may request the renewal of a certificate before it expires by sending to the appropriate RA an e-mail signed with the private key associated with the certificate for which renewal is requested.

### 4.6.3 Processing certificate renewal requests

Upon receipt of the request endorsed by the appropriate RA, the AUSTRIANGRID CA shall process the renewal as it processes an initial certification request.

### 4.6.4 Notification of new certificate issuance to subscriber

The AUSTRIANGRID CA shall notify the subscriber of the issuance as described for the initial certificate issuance in 4.3.2.

### 4.6.5 Conduct constituting acceptance of the renewal certificate

The same procedure shall be followed as described in 4.4.1.

### 4.6.6 Publication of the renewal certificate by the CA

See 4.4.2.

### 4.6.7 Notification of certificate issuance by the CA to other entities

See 4.4.3

## 4.7 Certificate re-key

### 4.7.1 Circumstance for certificate re-key

For security reasons, the certificate re-key is the preferred method for issuing a new certificate to a subscriber whose certificate is about to expire or who wants a change in the certificate parameters.

### 4.7.2 Who may request certification of a new public key

The owner of a valid certificate may request the certification of a new public key in a CSR also signed with his/her still valid private key.
If the certificate has already expired a certificate request procedure as described for an initial certification request must be followed.

#### 4.7.3 Processing certificate re-keying requests

Upon receipt of the request endorsed by the appropriate RA, the AUSTRIANGRID CA shall process the renewal as it processes an initial certification request.

#### 4.7.4 Notification of new certificate issuance to subscriber

The AUSTRIANGRID CA shall notify the subscriber of the issuance as described for the initial certificat issuance in 4.3.2.

#### 4.7.5 Conduct constituting acceptance of the re-keyed certificate

The same procedure shall be followed as described in 4.4.1.

#### 4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2.

#### 4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3

### 4.8 Certificate modification

#### 4.8.1 Circumstance for certificate modification

Certificates must not be modified. The old certificate must be revoked, and a new key pair must be generated and a request for the modified certificate contents submitted with the new public key. The revocation may be conditional on the issuance and acceptance of the new certificate, and thus the old certificate will only be revoked after the new one is accepted.

#### 4.8.2 Who may request certification modification

The owner of the original certificate may submit the requests for re-key and revocation as per 4.7.2 and 4.9.3 respectively.

#### 4.8.3 Processing certificate modification requests

Not applicable

#### 4.8.4 Notification of new certificate issuance to subscriber

Not applicable

#### 4.8.5 Conduct constituting acceptance of the modified certificate

Not applicable

#### 4.8.6 Publication of the modified certificate by the CA

Not applicable

#### 4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable

### 4.9 Certificate revocation and suspension

#### 4.9.1 Circumstances for revocation

A certificate must be revoked if:

- its associated private key has been (or is suspected to be) compromised or lost
- its contents have become or proved to be inaccurate
- it is not needed any more
- the consenting organisation/unit withdraws its consent

Should the private key of the AUSTRIANGRID CA be compromised or lost all certificates signed with it shall be revoked.

#### 4.9.2 Who can request revocation

The revocation request can be issued by

- the owner of the certified key
- the AUSTRIANGRID CA or any RA that has proof of a compromise
- the organisation/unit that wants to revoke its consent to its inclusion in the certificate

#### 4.9.3 Procedure for revocation request

Unless the AUSTRIANGRID CA acts on its own a revocation request must be made:

- by the owner of the certificate in an e-mail signed with the private key associated with the (still not expired) certificate,

- on behalf of the owner who has lost his/her private key in an e-mail signed by an authorised person of the organisation/unit that consented to the certificate, or
- on behalf of the organisation/unit that consented to the certificate in an e-mail signed by an authorised person (see 3.2.2)

In case of emergency if no such e-mail can be sent, the revocation can be initiated via oral communication with the appropriate RA or the AUSTRIANGRID CA. Before revoking a certificate the AUSTRIANGRID CA shall authenticate the source of the request according procedures as used for the initial registration.

#### 4.9.4 Revocation request grace period

No grace period shall be defined for a revocation request. The AUSTRIANGRID CA shall process the authenticated request with priority and publish the revocation as fast as possible.

#### 4.9.5 Time within which CA must process the revocation request

The AUSTRIANGRID CA must process revocation requests with the highest priority.

#### 4.9.6 Revocation checking requirement for relying parties

Before using a certificate the relying party must validate it against the CRL (or, later, using the planned OCSP facility) most recently published in the AUSTRIANGRID CA repository.

#### 4.9.7 CRL issuance frequency (if applicable)

A new CRL is published in the AUSTRIANGRID CA repository after every certificate revocation and at least 7 days before the expiration of the previous CRL.

#### 4.9.8 Maximum latency for CRLs (if applicable)

The CRL shall be copied to a removable device immediately after creation on the off-line CA system and transfered without delay to the on-line repository.

#### 4.9.9 On-line revocation/status checking availability

The AUSTRIANGRID CA shall publish the CRL in effect in its repository (see 2.1). No other on-line checking is available now, but it is planned to setup an OCSP facility).

#### 4.9.10 On-line revocation checking requirements

Relying parties must check the CRL before they use and trust a certificate.
No access control shall limit the possibility to check the CRL.

#### 4.9.11 Other forms of revocation advertisements available

Except for informing the owner of a newly revoked certificate and the appropriate RA of the issued revocation no advertisement of a new CRL other than its publication in the AUSTRIANGRID CA repository will be made.

#### 4.9.12 Special requirements re key compromise

No stipulation

#### 4.9.13 Circumstances for suspension

Not defined

#### 4.9.14 Who can request suspension

Not defined.

#### 4.9.15 Procedure for suspension request

Not defined.

#### 4.9.16 Limits on suspension period

Not specified

### 4.10 Certificate status services

#### 4.10.1 Operational characteristics

The AUSTRIANGRID CA shall store in its public repository and make them available via its web site:

- the root CA certificate,
- all valid certificates, and
- the most up-to-date CRL.

#### 4.10.2 Service availability

The AUSTRIANGRID CA shall run this service available continuously, except for unavoidable maintainance activities. Due to the nature of the Internet this service can't be guaranteed to be always accessible.

### 4.10.3 Optional features

It is planned that the AUSTRIANGRID CA will offer an OCSP service at a later date.

## 4.11 End of subscription

The subscription ends with the expiry of the certificate if it is not renewed before that date.
A subscription may end earlier if the subscriber requests it in an e-mail sent to the RA and signed by the subscriber, or if the sponsoring organisation or organisational unit asks for it in an e-mail signed by one of its agents and sent to the appropriate RA. The RA must authenticate the request and send it to the CA in an e-mail signed by one of its agents.
The AUSTRIANGRID CA shall revoke the certificate starting with the date mentioned in the request or the processing of the request, whichever is later. If no date is mentioned in the request, the date of the request is assumed.

## 4.12 Key escrow and recovery

### 4.12.1 Key escrow and recovery policy and practices

No key escrow or recovery services are provided. The key owner must take all steps to prevent a loss.

### 4.12.2 Session key encapsulation and recovery policy and practices

See 4.12.1

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 5.1 Physical Controls

### 5.1.1 Site location and construction

The AUSTRIANGRID CA is located at the address of the organisation administering this document (see 1.5.1).

### 5.1.2 Physical access

RA and CA machines are in a controlled environment where access is restricted to authorised personnel.

### 5.1.3 Power and air conditioning

The server room hosting the offline and the online AUSTRIANGRID CA servers have air conditioning. The servers are powered via a UPS that allows to bridge power outages of several minutes.

### 5.1.4 Water exposures

No special exposures.

### 5.1.5 Fire prevention and protection

No special provisions.

### 5.1.6 Media storage

Removable media shall be stored in locked safe places to which only authorised personnel have access.

### 5.1.7 Waste disposal

Waste containing data to be protected (cryptographically relevant data like private keys or passphrases, or personal data) shall be disposed off in a way to guarantee that the information may not be re-used.

### 5.1.8 Off-site backup

No provisions yet

## 5.2 Procedural Controls

### 5.2.1 Trusted roles

No provisions yet

### 5.2.2 Number of persons required per task

At least 3 people shall be able to perform CA operator tasks.

### 5.2.3 Identification and authentication for each role

### 5.2.4 Roles requiring separation of duties

Except for the management, no roles at the AUSTRIANGRID CA require separation of duties.
Information about a subscriber stored at the site of the AUSTRIANGRID CA and that is to be considered as private (see 9.4.2) shall only be accessible to the operators of the RA that administers that subscriber's requests.

## 5.3 Personnel Controls

### 5.3.1 Qualifications, experience, and clearance requirements

All AUSTRIANGRID CA personnel shall have system administrator or analyst experience.

### 5.3.2 Background check procedures

No provisions

### 5.3.3 Training requirements

All people acting as CA operators shall be trained on the job by the installer/maintainer of the CA software.

### 5.3.4 Retraining frequency and requirements

Retraining shall be mandatory when new software or features, as well as new organisational procedures are introduced.

### 5.3.5 Job rotation frequency and sequence

No stipulation

#### 5.3.6 Sanctions for unauthorized actions

The AUSTRIANGRID CA reserves the right to prosecute unauthorized actions to the extend provided by the provisions of the University of Vienna and the Austrian law.

#### 5.3.7 Independent contractor requirements

No stipulation

#### 5.3.8 Documentation supplied to personnel

All AUSTRIANGRID CA personnel shall be provided with all documentation required for successfully performing their task.

### 5.4 Audit logging procedures

#### 5.4.1 Types of event recorded

The following events shall be recorded :

- on the offline certification host
  - boot and shutdown
  - logins and logouts
  - creation and signing of certificates
- on the online AUSTRIANGRID CA server
  - receipt of certificate requests from an RA
  - insertion of data in the AUSTRIANGRID CA data base
  - transfer of certificate request to removable medium
  - transfer of certificate to requesting party
  - storage of certificate in online repository
  - receipt of revocation request
  - CRL issues

#### 5.4.2 Frequency of processing log

The log files shall be analysed once a month, or after a potential security breach is suspected or known; whichever comes first.

#### 5.4.3 Retention period for audit log

The minimal retention period for the audit logs is 3 years.

#### 5.4.4 Protection of audit log

The audit logs shall only be accessible to the AUSTRIANGRID CA operators and managers. The protection shall be state-of-the-art best effort.

#### 5.4.5 Audit log backup procedures

The audit logs shall be backed-up on a removable medium every night except on weekends and holidays when no activity happens on the offline host and only read access to the online repositories happens on the online server.

#### 5.4.6 Audit collection system (internal vs external)

internal

#### 5.4.7 Notification to event-causing subject

Not defined

#### 5.4.8 Vulnerability assessments

Not defined.

### 5.5 Records Archival

#### 5.5.1 Types of event recorded

See 5.4.1

#### 5.5.2 Retention period for archive

The minimum retention period is 3 years.

#### 5.5.3 Protection of archive

The archive shall be accessible to the AUSTRIANGRID CA operation and management personnel only.

#### 5.5.4 Archive backup procedures

Records shall be backed up on removable media, which shall be stored in a room with restricted access.

#### 5.5.5 Requirements for time-stamping of records

All event records shall bear a time-stamp.

### 5.5.6 Archive collection system (internal or external)

The archive shall be stored on the online system containing the AUSTRIANGRID CA repository. It shall be protected on a best effort-basis.

### 5.5.7 Procedures to obtain and verify archive information

Not defined

## 5.6 Key changeover

As the key generation is done by each entity for its own use, no provision is made for a key changeover.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and compromise handling procedures

### 5.7.2 Computing resources, software, and/or data are corrupted

If the keys of an end entity are lost or compromised due to corruption of their computing basis, the appropriate RA has to be informed immediately in order to start the certificate revocation process.
In case this happens to an RA the CA has to be informed without delay. All of their certificates shall be revoked immediately. The CA together with the RA shall start without delay investigating the damage to and loss of information stored at the RA in order to minimise the impact on all end entities and relying parties concerned.
In order to be able to resume operation as fast as possible after the compute basis of the CA is corrupted the following steps shall be performed:

- All CA software shall be backed-up on removable media after a new release of any of its components is installed.
- All data files of the offline CA shall be backed-up on a removable medium after each change, before the session is closed.

In case of corruption of any part of the running system, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a read-only medium and estimated to be uncorrupted. If not all encrypted copies of the AUSTRIANGRID CA private key are destroyed or lost, and are not compromised, the operation shall be re-established as soon as possible without need to revoke all issued certificates.

### 5.7.3 Entity private key compromise procedures

In case the key of an end entity or an RA is compromised, the corresponding certificate must be revoked. All relying parties known to accept the key should be

informed by the owner of the key.
In case the private key of the AUSTRIANGRID CA is compromised (or suspected to be) the CA shall:

- make every reasonable effort to notify subscribers and RAs,
- terminate issuing and distributing certificates and CRLs,
- request revocation of the compromised certificate,
- generate a new CA key pair and certificate and publish the certificate in the repository,
- revoke all certificates signed using the compromised key, and
- publish the new CRL on the AUSTRIANGRID CA repository.

### 5.7.4 Business continuity capabilities after a disaster

Not defined

## 5.8 CA or RA Termination

In case of termination of its services AUSTRIANGRID CA will:

- make all reasonable efforts to inform subscribers and RAs as soon as possible,
- announce the termination as widely as possible,
- cease issuing certificates,
- revoke all certificates, and
- destroy all copies of private keys of AUSTRIANGRID CA.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key pair generation

The key pair for the AUSTRIANGRID CA is generated by authorized CA staff on a computer which is not connected to the network. The keys are generated by software using OpenSSL.
The key pairs for natural-person (including RA agents), host or service certificates are generated by the requesting parties themselves on their system.

### 6.1.2 Private key delivery to subscriber

Each requesting party must generate its own key pair.

### 6.1.3 Public key delivery to certificate issuer

The RA authenticating the requests transmits the the certification requests containing the public key in an e-mail signed by one of its agents.

### 6.1.4 CA public key delivery to relying parties

The AUSTRIANGRID CA certificate can be downloaded from the repository (see 2.1)

### 6.1.5 Key sizes

The key shall be an RSA key with a modulus of at least 1024 bit. For the AUSTRIANGRID CA the key shall be an RSA key with a modulus of 2048 bit.

### 6.1.6 Public key parameters generation and quality checking

Not defined.

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

The keys may be used according to the type of certificate:

- with an end-entity certificate for
    - authentication,
    - non-repudiation,
    - data and key encypherment,
    - checking the integrity of objects, especially messages,
    - session establishment,

- proxy creation and signing (according to [21])

- with an RA certificate for
  - all activities needed for the work of an RA agent
- with an OCSP certificate for
  - signing of OCSP responses
- with the self-signed CA certificate
  - certificate signing
  - CRL signing

## 6.2 Private Key Protection and Cryptographic Module Engineering

### 6.2.1 Cryptographic module standards and controls

End entities shall use the web form available on the AUSTRIANGRID CA web site for key and CSR generation, whenever possible. If this is not possible. proven technologies for key creation that are not less sophisticated than what OpenSSL provides must be used, and the CA must check their suitability and agree with them.
The CA private key is generated using OpenSSL.
Each CA operator shall have his own personal copy of the CA private key encrypted with a passphrase of at least 12 characters and only known to him. These encrypted private keys shall be stored on the offline computer of the AUSTRIANGRID CA.
An extra instance of the private key encrypted with a randomly generated passphrase of at least 12 characters shall be stored on removable media which must be deposited in a safe and locked up place; the passphrase shall be stored on a different removable media or written down, and the media or paper shall be placed in a sealed envelop and stored in a different secure place.
No instance of the private CA key (plain or encrypted) shall reside on the permanent disc of any computer that is online.

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

This type of control is not yet installed.

### 6.2.3 Private key escrow

No key escrow service is planed.

### 6.2.4 Private key backup

Subscribers are responsible for the backup of their encrypted private keys.
The instance of the private CA key encrypted with the random key and the copy of the passphrase serve as backup.

### 6.2.5 Private key archival

No stipulation

### 6.2.6 Private key entry into or from cryptographic module

In order to perform certification activities the private CA key encrypted with the operators personal passphrase stored on the off-line certification server must be used and activated.

### 6.2.7 Method of activating private key

The CA private key is activated by having the CA operator enter his personal passphrase.

### 6.2.8 Method of deactivating private key

The plain private key shall only be stored in RAM and erased when the activity for which it is needed is finished.

### 6.2.9 Method of destroying private key

See above.

### 6.2.10 Cryptographic module rating

No stipulation

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public key archival

The AUSTRIANGRID CA shall archive all certificates it has ever issued on removable media that is stored off-line in a secure place.

### 6.3.2 Certificate operational periods and key pair usage periods

There is no stipulation as to the validity of the generated key pair. Only the validity of the certificate issued by the AUSTRIANGRID CA is defined by this CP/CPS document.
The default end-entity and RA certificate lifetime is 395 days (approximately one

year plus one month). A shorter lifetime may be requested, e.g. if it is known that the affiliation of the requesting party to the group participating in the AUSTRIAN GRID will be less than 13 months.
The AUSTRIANGRID CA certificate has a lifetime of 5 years.

## 6.4 Activation Data

### 6.4.1 Activation data generation and installation

Each private key shall be protected by a passphrase which consists of at least 12 characters.

### 6.4.2 Activation data protection

The passphrase must only be known to the person who owns the encrypted private key. Any backup of the private key passphrase ((machine readable or on paper) must be stored in secured place.

### 6.4.3 Other aspects of activation data

Not defined

## 6.5 Computer Security Controls

### 6.5.1 Specific computer security technical requirements

All CA computers shall be based on Unix-like operating systems.
All sessions must be authenticated by using passwords or proxy certificates for login. The passwords (even in encrypted form) must not be accessible from other computer systems (e.g. through the use of the shadow password facility).

### 6.5.2 Computer security rating

Not defined

## 6.6 Life cycle technical controls

Not defined

### 6.6.1 System development controls

No stipulation.

### 6.6.2 Security management controls

No stipulation

### 6.6.3 Life cycle security controls

No stipulation.

## 6.7 Network Security Controls

The signing machine is kept offline.
All other CA computers are protected by a firewall and/or by removing all unnecessary services.

## 6.8 Time stamping

All time stamping of entries created on the online servers at the AUSTRIANGRID CA is based on the network time provided by the time server of the ZID of the University of Vienna.
The hardware clock of the offline system for the certificate and CRL signing which determines the time stamping of the certificates and the CRLs should be synchronized using a DCF77 or GPS module.

# 7 CERTIFICATE, CRL AND OCSP PROFILES

## 7.1 Certificate Profile

All certificates issued by the AUSTRIANGRID CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280 [3].

### 7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by the AUSTRIANGRID CA.

### 7.1.2 Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in the AUSTRIANGRID CA certificates are:

- for natural-person certificates:
  - standard extensions
    - Basic Constraints: `CRITICAL CA:FALSE`
    - Authority Key Identifier: composed of the 160-bit SHA-1 hash of the value of the public key of the certificate issuer
    - Subject Key Identifier: composed of the 160-bit SHA-1 hash of the value of the certified public key
    - Key Usage: `CRITICAL` values:
      - digitalSignature,
      - nonRepudiation,
      - keyEncypherment,
      - dataEncypherment,
      - keyAgreement,
    - Extended Key Usage: `CRITICAL` values:
      - clientAuth
      - codeSigning
      - emailProtection
      - timeStamping
    - Certificate Policies: OID of the CP/CPS document in effect at the time of issuance of the certificate
    - Subject Alternative Name: for a certificate issued to a natural person the e-mail address relevant for any communication with the end entity as cited in this CP/CPS document
    - Issuer Alternative Name: link (URI) to the issuer's certificate
    - CRL Distribution Points: URI of the CRL, no ReasonFlags shall be set (in conformance with 7.2.2)

- Netscape Cert Extensions:
  - netscape-cert-type:
    - SSL Client
    - S/MIME
    - Object Signing

- for automated-system and service/application certificates:
  - standard extensions
    - Basic Constraints: `CRITICAL CA:FALSE`
    - Authority Key Identifier: composed of the 160-bit SHA-1 hash of the value of the public key of the certificate issuer
    - Subject Key Identifier: composed of the 160-bit SHA-1 hash of the value of the certified public key
    - Key Usage: `CRITICAL` values:
      - digitalSignature,
      - nonRepudiation,
      - keyEncypherment,
      - dataEncypherment,
      - keyAgreement,
    - Extended Key Usage: `CRITICAL` values:
      - serverAuth
      - clientAuth
      - codeSigning
      - emailProtection
      - timeStamping
    - Certificate Policies: OID of the CP/CPS document in effect at the time of issuance of the certificate
    - Subject Alternative Name: the fully qualified domain name (FQDN) of the host
    - Issuer Alternative Name: link (URI) to the issuer's certificate
    - CRL Distribution Points: URI of the CRL, no ReasonFlags shall be set (in conformance with 7.2.2)
  - Netscape Cert Extensions:
    - netscape-cert-type:
      - SSL Server
      - SSL Client
      - S/MIME
      - Object Signing

- for the self signed CA certificate used only for certificate and CRL signing:
  - standard extensions
    - Basic Constraints: `CRITICAL CA:TRUE`
    - Authority Key Identifier: composed of the 160-bit SHA-1 hash of the value of the public key of the certificate issuer
    - Subject Key Identifier: composed of the 160-bit SHA-1 hash of the value of the certified public key
    - Key Usage: `CRITICAL` values:
      - keyCertSign,
      - cRLSign
    - Certificate Policies: OID of the CP/CPS document in effect at the time of issuance of the certificate
    - CRL Distribution Points: URI of the CRL, no ReasonFlags shall be set (in conformance with 7.2.2)
  - Netscape Cert Extensions:
    - netscape-cert-type:
      - SSL CA
      - S/MIME CA
      - Object Signing CA
- for CA certificates for all other purposes:
  - standard extensions
    - Basic Constraints: `CRITICAL CA:FALSE`
    - Authority Key Identifier: composed of the 160-bit SHA-1 hash of the value of the public key of the certificate issuer
    - Subject Key Identifier: composed of the 160-bit SHA-1 hash of the value of the certified public key
    - Key Usage: `CRITICAL` values:
      - digitalSignature,
      - nonRepudiation,
      - keyEncypherment,
      - dataEncypherment,
      - keyAgreement,
    - Extended Key Usage: `CRITICAL` values:
      - serverAuth
      - clientAuth
      - codeSigning
      - emailProtection

            - timeStamping
        - Certificate Policies: OID of the CP/CPS document in effect at the time of issuance of the certificate
        - Issuer Alternative Name: link (URI) to the issuer's certificate
        - CRL Distribution Points: URI of the CRL, no ReasonFlags shall be set (in conformance with 7.2.2)
    - Netscape Cert Extensions:
        - netscape-cert-type:
            - SSL Server
            - SSL CA
            - S/MIME
            - S/MIME CA
            - Object Signing
            - Object Signing CA

- for OCSP certificates (as defined in [22]):
    - standard extensions
        - Basic Constraints: `CRITICAL CA:FALSE`
        - Authority Key Identifier: composed of the 160-bit SHA-1 hash of the value of the public key of the certificate issuer
        - Subject Key Identifier: composed of the 160-bit SHA-1 hash of the value of the certified public key
        - Key Usage: `CRITICAL` values:
            - digitalSignature,
            - nonRepudiation,
            - keyEncypherment,
            - dataEncypherment,
            - keyAgreement,
        - Extended Key Usage: `CRITICAL` values:
            - serverAuth
            - timeStamping
            - OCSPSigning
        - Certificate Policies: OID of the CP/CPS document in effect at the time of issuance of the certificate
        - Issuer Alternative Name: link (URI) to the issuer's certificate
        - authorityInfoAccess: URI of the OCSP responder
    - Netscape Cert Extensions:
        - netscape-cert-type:
            - SSL Server

- SSL CA
- S/MIME
- S/MIME CA
- Object Signing
- Object Signing CA

### 7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by the AUSTRIANGRID CA are according to [12]:

- hash function: id-sha1 — 1.3.14.3.2.26
- encryption: rsaEncryption — 1.2.840.113549.1.1.1
- signature: sha-1WithRSAEncryption — 1.2.840.113549.1.1.5

### 7.1.4 Name forms

Each entity has a unique and unambiguous Distinguished Name (DN) in all the certificates issued to the same entity by the AUSTRIANGRID CA. The DN shall be structured as defined in ITU-T Standards Recommendation X.501. [20]

Depending on the type of entity the DN has the following form:

- `C=AT`
- `O=AustrianGrid`
- `OU=`*unit* This entry may be used recursively
  - each organisation may define the hierarchy to be used
  - the first entry denotes the organisation to which the entity belongs
  - the following OU entries describe the units and sub-units (e.g. institute, department or project)
  - for an RA the last OU entry shall be `Registration Authority`
- `CN=`*common name* Depending on the type of the entity the common name shall be:
  - for a natural person: first-name last-name (optionally an extension to make the name unique within the organisational unit)
  - for an automated system: the Fully Qualified Domain Name (FQDN)
  - for a service: the service name followed by a slash (“/”) and the FQDN of the automated system it is running on

  - for the RAs: CN of the authorised natural person who is acting as agent for the RA (each RA agent uses his/her own key pair certified for RA activities)

- the DN of the AUSTRIANGRID CA certificate issuer shall be:
  `C=AT/O=AustrianGrid/OU=Certification Authority/CN=Certificate Issuer`

In order to be able to recognise the type of entity the CN of a natural person must not contain a slash ("/") anywhere and must not contain a period (".") before the first white space

#### 7.1.5 Name constraints

There are no other name constraints than those that are to be derived from the stipulations in 7.1.4, 3.1.2 and 3.1.1.

#### 7.1.6 Certificate policy Object Identifier

The OID of this CP is: 1.3.6.1.4.1.21356.1.1.1.2.0.

#### 7.1.7 Usage of Policy Constraints extension

No stipulation

#### 7.1.8 Policy qualifiers syntax and semantics

No stipulation

#### 7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation

### 7.2 CRL Profile

#### 7.2.1 Version number(s)

The AUSTRIANGRID CA shall create and publish X.509 version 2 CRLs.

#### 7.2.2 CRL and CRL entry extensions

The AUSTRIANGRID CA shall issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation shall not be included in the individual CRL entries.
The CRL shall include the date by which the next CRL shall be issued. A new CRL shall be issued before this date if new revocations are issued.
The CRL extensions that shall be included are:

- the Authority Key Identifier (equal to the issuer's key identifier)
- the CRL Number (a monotonically increasing sequence number)

No CRL entry extensions will be used.

## 7.3 OCSP profile

### 7.3.1 Version number(s)

OCSP profiles version 1 shall be be used in requests and responses.

### 7.3.2 OCSP extensions

Not yet defined

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

## 8.1 Frequency and circumstances of assessments

The AUSTRIANGRID CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.
The CA shall at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect.

## 8.2 Identity/qualifications of assessor

Not defined

## 8.3 Assessor's relationship to assessed party

The assessments are made by personnel of the AUSTRIANGRID CA or members of the AUSTRIAN GRID consortium.
If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of AUSTRIANGRID CA's personnel and infrastructure.

## 8.4 Topics covered by assessment

Not defined

## 8.5 Actions taken as result of deficiency

The AUSTRIANGRID CA shall take immediate action if the assessment reveals a conflict between the provisions of the CP/CPS document and the actual practice. This may result in improving the practice with, potentially, reflecting the change in a new version of the CP/CPS document, or if the practice seems adequate the policy and CP/CPS document shall be reviewed.
If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

## 8.6 Communication of results

The results of the assessment shall be summed up in a protocol agreed by the assessor and the AUSTRIANGRID CA. If no agreement can be reached each party may compile its own version; any communication of results must then provide both versions.
The distribution of the protocol or parts of it shall be jointly defined by the assessor and the AUSTRIANGRID CA management according to need-to-know criteria.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

No fees are charged for services to the AUSTRIAN GRID consortium.

### 9.1.1 Certificate issuance or renwal fees

See 9.1

### 9.1.2 Certificate access fees

See 9.1

### 9.1.3 Revocation or status information access fees

See 9.1

### 9.1.4 Fees for other services

See 9.1

### 9.1.5 Refund policy

See 9.1

## 9.2 Financial responsibility

No financial responsibility is accepted

### 9.2.1 Insurance coverage

No stipulation

### 9.2.2 Other assets

No stipulation

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

No stipulation

### 9.3.2 Information not within the scope of confidential information

No stipulation

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

No stipulation

### 9.4.2 Information treated as private

The Austrian law on privacy (Datenschutzgesetz) defines the minimum extent of what shall be considered information to be treated as private.
Furthermore all information about subscribers that is not included in the certificates and CRL shall be considered confidential and shall not be released outside the AUSTRIANGRID CA and the RA performimg the registration.

### 9.4.3 Information not deemed private

Information included in the certificates and the CRL issued by the AUSTRIANGRID CA shall not be considered private. By requesting a certificate from the AUSTRIANGRID CA the subscriber consents to the inclusion of this information as part of the certificate publication.

### 9.4.4 Responsibility to protect private information

The responsibility to protect private information rests with the AUSTRIANGRID CA and all its accredited RAs.

### 9.4.5 Notice and consent to use private information

In case the AUSTRIANGRID CA or any of its accredited RAs wants to use private information it must ask the subscriber for a written consent. No subscriber shall be under the impression that he/she has an obligation to agree.

### 9.4.6 Disclosure persuant to judicial or administrative process

Persuant to a judicial or administrative process private information shall only be released upon presentation of a regular warrant issued according to the Austrian law.

### 9.4.7 Other information disclosure circumstances

No stipulation

## 9.5 Intellectual property rights

The AUSTRIANGRID CA does not claim any IPR on certificates, policy/practice specifications, names and keys.

Parts of this document are inspired or even copied from the CP/CPS documents of CERN [13], CNRS [14], the German Grid [15], IUCC [16], the Dutch Grid [17], SWITCH [18] and UK eScience [19], and may-be indirectly from documents they draw from.
Anybody may freely copy any parts of this CP/CPS document provided they include an acknowledgement of the source.
This document was typeset with LaTeX.

## 9.6 Representations and warranties

### 9.6.1 CA representations and warranties

The information published in the certificates, CRLs and OCSP responses are accurate to the best of AUSTRIANGRID CA's knowledge. No other warranties are accepted.

### 9.6.2 RA representations and warranties

All accredited RAs shall perform their task of identification of the requesting parties as described in 3.2.3 and 3.2.2 to the best of their knowledge. No other warranties are accepted.
An RA can conclude, at its strictly own risk, a more stringent agreement with its subscribers, but this shall never commit the AUSTRIANGRID CA nor any of its other accredited RAs.

### 9.6.3 Subscriber representations and warranties

By requesting an AUSTRIANGRID CA certificate a subscriber commits itself to use and protect the certificate and the certified keys according to the stipulations of the CP/CPS document in effect at the date of issuance of the said certificate. (S)he may however apply more stringent observances.
In particular the subscriber shall inform the AUSTRIANGRID CA without delay if the private key associated with a certificate issued by the AUSTRIANGRID CA is lost or compromised so that the certificate can be revoked and relying parties refuse to accept it.
In case of a breach of stipulations of the CP/CPS document that the subscriber has agreed to by requesting the AUSTRIANGRID CA certificate the certificate shall be revoked immediately. No further warranties are required from the subscriber.

### 9.6.4 Relying party representations and warranties

A relying party shall check the validity of any certificate that claims issuance by the AUSTRIANGRID CA against the self-signed certificate of the CA and the CRL in effect at the time of the intended acceptance.

When it issues a proxy based on a certificate issued by the AUSTRIANGRID CA a relying party should take all possible measures to limit the damage caused by a proxy outliving the validity of a certificate on which it is based directly or through one or more intervening proxies ([21]).

### 9.6.5 Representations and warranties of other participants

No stipulation

## 9.7 Disclaimers of warranties

The AUSTRIANGRID CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness.
Also the AUSTRIANGRID CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.
Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

## 9.8 Limitations of liability

Except if dictated otherwise by the Austrian law the AUSTRIANGRID CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.
It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.

## 9.9 Indemnities

The AUSTRIANGRID CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.
End entities shall idemnify and hold harmless the AUSTRIANGRID CA and all appropriate RAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP/CPS document.

## 9.10 Term and termination

### 9.10.1 Term

This document becomes effective after its publication on the Web site of the AUSTRIANGRID CA starting at the date announced there.
No term is set for its expiration.

### 9.10.2 Termination

This CP/CPS remains effective until it is superseeded by a newer version.

### 9.10.3 Effect of termination and survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

## 9.11 Individual notices and communications with participant

All e-mail communications between the CA and its accredited RAs must be signed with a certified key.
All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

## 9.12 Amendments

### 9.12.1 Procedure for amendments

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

### 9.12.2 Notification mechanism and period

The amended CP/CPS document shall be published on the AUSTRIANGRID CA Web pages at least 2 weeks before it becomes effective.
The AUSTRIANGRID CA will inform its subscribers and all relying parties it knows of by means of an e-mail.

### 9.12.3 Circumstances under which OID must be changed

Substantial changes shall cause the OID to be changed. The decision is made by the manager of the AUSTRIANGRID CA and submitted to the AUSTRIAN GRID PMA for approval.

## 9.13 Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the manager of the AUSTRIANGRID CA.

## 9.14 Governing law

The AUSTRIANGRID CA and its operation are subject to the Austrian law. All legal disputes arising from the content of this CP/CPS document, the operation of the AUSTRIANGRID CA and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by AUSTRIANGRID CA shall be treated according to Austrian law.

## 9.15 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of an AUSTRIANGRID CA certificate must comply with the Austrian law.
Activities initiated from or destined for another country than Austria must also comply with that country's law.

## 9.16 Miscellaneous provisions

### 9.16.1 Entire agreement

This CP/CPS document superseeds any prior agreements, written or oral, between the parties covered by this present document.

### 9.16.2 Assignment

No provisions

### 9.16.3 Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

No provisions

### 9.16.5 Force Majeure

Events that are outside the control of the AUSTRIANGRID CA will be dealt with immediately by the PMA.

### 9.17 Other provisions

No stipulation

# References

[1] S. Chokani, W. Ford, R. sabett and S. Wu “Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework”, RFC 3647, November 2003 - http://www.ietf.org/rfc/rfc3647.txt

[2] S. Chokani and W. Ford, “Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework”, RFC 2527, March 1999 - http://www.ietf.org/rfc/rfc2527.txt

[3] R. Housley, W. Polk, W. Ford and D. Solo, “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”, RFC 3280, April 2002 - http://www.ietf.org/rfc/rfc3280.txt

[4] R. Housley, W. Ford, W. Polk and D. Solo, “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile”, RFC 2459, April 1999 - http://www.ietf.org/rfc/rfc2459.txt

[5] Austrian Grid - http://www.austriangrid.at
AustrianGrid CA - http://www.austriangridca.at

[6] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999 with all amendments, see: http://www.signatur.rtr.at/de/legal/sigg.html

[7] DIRECTIVE 199/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, p. 12 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF

[8] S. Brader, “Key words for use in RFCs to Indicate Requirement Levels”, RFC 2119, March 1997 - http://www.ietf.org/rfc/rfc2119.txt

[9] M. Nystrom and B. Kaliski, “PKCS #10: Certification Request Syntax Specification Version 1.7”, RFC 2986, November 2000 - http://www.ietf.org/rfc/rfc2986.txt

[10] J. Case, M. Fedor, M. Schoffstall and J. Davin, “A simple Network Management Protocol (SNMP)”, RFC 1157, May 1990 - http://www.ietf.org/rfc/rfc1157.txt

[11] D. Crocker, “Standard for the format of ARPA Internet text messages”, RFC 822, August 1982 - http://www.ietf.org/rfc/rfc822.txt

[12] W. Polk, R. Housley and L. Bassham, “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002 - http://www.ietf.org/rfc/rfc3279.txt

[13] CERN Certification Authority Certificate Policy and Certification Practice Statement, Version 2.2, March 2004 - https://edms.cern.ch/file/431705/3/CP-CPS.pdf

[14] Certificate Policy and Certification Practice Statement CNRS/CNRS-Projets/Datagrid-fr, Version 0.3, August 2002 - http://www.urec.cnrs.fr/igc/Doc/Datagrid-fr.policy.pdf

[15] Forschungszentrum Karlsruhe in der Helmholtz-Gemeinschaft GridKa-CA Certificate Policy and Certification Practice Statement, Version 1.1, July 2004 - http://grid.fzk.de/ca/gridka-cps.pdf

[16] IUCC Certification Authority Certificate Policy and Certification Practice Statement, Draft Version 1.5, December 2003 - http://certificate.iucc.ac.il/ca/IUCC_CP-CPS_1_5.pdf

[17] DutchGrid and NIKHEF Medium-security X.509 Certification Authority Certificate Policy and Certification Practice Statement, Version 2.1, November 2001 - http://certificate.nikhef.nl/medium/policy/cps-medium-2.1.pdf

[18] SWITCH Certificate Policy and Certification Practice Statement, Version 1.0, 2004 - http://www.switch.ch/pki/SWITCH_CP-CPS200401.pdf

[19] UK eScience Certification Authority Certificate Policy and Certification Practices Statement, Version 1.0, October 2003 - http://www.grid-support.ac.uk/ca/cps/cps-1.0.pdf

[20] TU-T Recommendation X.501: Information Technology - Open Systems Interconnection - The Directory: Models, 1993

[21] S. Tuecke, V. Welch, D. Engert, L. Pearlman and M. Thompson, “Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile”, RFC 3820, June 2004 – http://www.ietf.org/rfc/rfc3820.txt

[22] M. Myers, R. Ankey, A. Malpani, S. Galperin and C. Adams, “X.509 Internet Public Key Infrastracture Online Certificate Status Protocol - OCSP”, RFC 2560, June 1999 - http://www.ietf.org/rfc/rfc2560.txt