UGRID
Ukrainian National Grid
Certification Authority

Certificate Policy
and
Certification Practice Statement

Version 1.4 draft
Document OID: 1.2.840.113612.5.4.2.6.1.1.1.4

December 2007

1. INTRODUCTION

1.1 Overview

The UGRID project goals are

- creation of a national Ukraine Grid-infrastructure;
- integrate UGRID with European Grid-infrastructure, take an active part in the formation of new European Grid concept (EGI);
- organize dissemination events in the society to enhance knowledge about Grid technology and skills of Grid using which will help national scientists and researchers to design and develop applications on Grid-infrastructure;
- provide efficient collaborative using of the computers, unique experimental equipments and devices, scientific data of researchers.
- take a part in the FP7 with the help and support of the EGI.

The Ukraine Grid Certification Authority is created to provide the needs of Ukrainian research and education community for Public Key Infrastructure service, as well as to allow integration UGRID infrastructure with European and World Grids.

The *UGRID CA* is hosted and operated at the High-Performance Computing Center of the National Technical University of Ukraine "Kyiv Polytechnic Institute". The *UGRID CA* is supported by and works in collaboration with the government institutions and non-government organizations related to the IT sector.

The current Certificate Policy and Certification Practice Statement (CP/CPS or "the Policy") document defines the rules and operational procedures followed by the *UGRID CA*, including the minimum requirements and obligations for the issuance and management of certificates. It is structured in accordance with the layout set in IETF RFC 3647.

1.2 Document name and identification

Document title	The UGRID CA Certificate Policy and Certification Practice Statement
Document version	Version 1.4
Document date	13.12.2007.
ASN.1 Object Identifier (OID)	1.2.840.113612.5.4.2.6.1.1.1.4

1.3 PKI participants

1.3.1 Certification Authorities

The UGRID CA is defined as a medium assurance CA. The UGRID CA does not issue certificates to subordinate Certification Authorities. The UGRID CA issue certificates under the approved versions of this CP/CPS document. Distribution of the validation process shall be implemented using a network of trusted Registration Authorities (RAs).

1.3.2 Registration Authorities

The procedures of verification of the Subscriber's identity and of approving their certificate requests are performed by trusted individuals – Registration Authorities. Such trusted intermediaries are formally assigned by the UGRID *CA*, their identities and contact details are published in the online repository (as described in section **2.2**), and the information is updated regularly. The RAs are required to declare their understanding of and adherence to this CP/CPS, and to perform their functions in accordance with it.

RAs do not issue certificates.

1.3.3 Subscribers

Certificates may be issued both to individuals and to computer entities. Eligible for certification by the UGRID *CA* are individuals or computer entities working for organizations formally based in and/or having offices inside the Ukraine, which are involved in the research and/or deployment of multi-domain distributed computing infrastructure, intended for cross-organizational sharing of resources, and/or which are participating actively in national and international Grid projects. This also includes services or host applications running on the referred computer entities; however, a host certificate shall be preferred to a service one in all cases where the latter is not strictly required. The focus of these organizations SHOULD also be in research and/or education.

1.3.4 Relying parties

All entities (including users of the Grid computing infrastructures) that employ the public keys in certificates, issued by the *UGRID CA*, for signature verification and/or encryption will be considered as relying parties.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate usage

The certificates issued by the *UGRID CA* may be used for any application that is suitable for X.509 certificates (e.g. e-mail signing and encryption (S/MIME), authentication and encryption of communications (SSL/TLS), network layer encryption (IPsec), object-signing, etc.), explicitly excluding the applications described in the following section.

1.4.2 Inappropriate certificate usage

Usage of the certificates issued by the *UGRID CA* for financial transactions or in violation of the Ukraine or international law is strictly forbidden.

1.5 Policy administration

1.5.1 Organization administering the document

The *UGRID CA* CP/CPS is authored and administered by the High-Performance Computing Center of the National Technical University of Ukraine “Kyiv Polytechnic Institute”.
The address of the *UGRID CA* for operational issues is:

CERTIFICATION AUTHORITY
High-Performance Computing Center
National Technical University of Ukraine “Kyiv Polytechnic Institute”
37, Prospect Peremohy,
03056, Kyiv-56,
Ukraine
Phone: +380444068013
Fax: +380444068013
Email: ca@ugrid.org

1.5.2 Contact Person

The contact person for questions about this CP/CPS document or any other the *UGRID CA* related issues is:
Velichkevych V. Sergiy

High-Performance Computing Center
National Technical University of Ukraine “Kyiv Polytechnic Institute”
37, Prospect Peremohy,
03056, Kyiv-56,
Ukraine
Phone: +380444068013
Fax: +380444068013
Email: serg@ugrid.org

1.5.3 Person determining CPS suitability for the policy

The person determining the CPS suitability for the policy is:

Velichkevych V. Sergiy
High-Performance Computing Center
National Technical University of Ukraine “Kyiv Polytechnic Institute”
37, Prospect Peremohy,
03056, Kyiv-56,
Ukraine
Phone: +380444068013
Fax: +380444068013
Email: serg@ugrid.org

1.5.4 CPS approval procedures

The approved document shall be submitted to EUGridPMA for acceptance and accreditation.

1.6 Definitions and acronyms

The following definitions and acronyms are used in this document:

Authentication	Authentication is the process of identifying a user. Usernames and passwords are the most common method of authentication
Certificate	Information issued by a trusted third party. Used to identify an individual or a system. Contains at least a subject, a unique serial number, an issuer and a validity period.
Certificate Authority	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certificate Extension	Optional fields in a certificate.

Certificate Policy	Rules that a request must comply with for the RA to approve the request or a CA to issue the certificate.
Certificate Revocation List	List of certificates that have been declared invalid. This list is issued by the CA at a regular interval and is used by applications to verify if a certificate is to be trusted.
Certification Practice Statement	Document that regulates rights and responsibilities of all the parties involved (RA, CA, directory service, end entity, relying party)
Certification Service Provider	Individual or corporation that issues certificates to individual or corporate third parties.
CP	⇒ Certificate Policy
CPS	⇒ Certification Practice Statement
Credentials	Evidence or testimonials concerning the user's right to access certain systems (e.g. username, password, etc)
CRL	⇒ Certificate Revocation List
CSP	⇒ Certification Service Provider
Distinguished Name	⇒ Subject
DN	⇒ Distinguished Name
Extension	Optional fields in a X509 Certificate.
Identity Provider (IdP)	(Shibboleth term.) Authority responsible for generating and asserting authentication, authorization, and identity information about their users in a security domain. This means the Identity Provider • registers its users and stores information about them • is able to authenticate their users
OCSP	Online Certificate Status Protocol: method to verify in real-time if a certificate is valid.
Participants	Entities like CAs, RAs, and repositories. These can be different legal entities.
PKI	⇒ Public Key Infrastructure
Private Key	One of two keys used in public key cryptography. The private key is known only to the owner and is used to sign and decrypt messages. The private key of a public-private key cryptography system. This key is used to “sign” outgoing messages, and is used to decrypt incoming messages.
Public Key	One of two keys used in public key cryptography. The public key can be known to anyone and is used to verify signatures and encrypt messages. The public key of a public-private key cryptography system. This key is used to confirm “signatures” on incoming messages or to

	encrypt a file or message so that only the holder of the private key can decrypt the file or message.
Public Key Infrastructure	Processes and technologies used to issue and manage digital identities for the use of third parties to authenticate individuals. Abbrev. PKI.
RDN	⇒ Relative Distinguished Name
Relative Distinguished Name	⇒ Subject
Revocation	Invalidation of a certificate. Every CA regularly issues a list of revoked certificates called CRL. This list should be verified by all applications that use certificates from that CA before trusting a certificate.
Rollover	To rollover a certificate means that a new certificate is issued while the old is still valid and usable. This is used to issue a new CA certificate while keeping the old valid and all the certificates that were issued with it.
Service Provider (SP)	A collection of Resources. However, since most Service Providers contain only one Resource, the term Service Provider is often used as synonym for Resource, although more in a technical sense.
Signature	Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
SSO	Single Sign On. The user only needs to login once to access various services.
Subject	Field in the Certificate that identifies the owner of the certificate. Also referred to as distinguished name (DN). The DN is composed of several fields, called relative distinguished names (RDN), which have the structure *variable_abbreviation=value*.

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.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All the online and off-line repositories of the *UGRID CA* are operated by the High-Performance Computing Center of the National Technical University of Ukraine "Kyiv Polytechnic Institute".

The address of the *UGRID CA* for issues regarding the repositories is:

CERTIFICATION AUTHORITY
High-Performance Computing Center
National Technical University of Ukraine "Kyiv Polytechnic Institute"
37, Prospect Peremohy,
03056, Kyiv-56,
Ukraine
Phone: +380444068013
Fax: +380444068013
Email: repositories@ugrid.org

2.2 Publication of certification information

The *UGRID CA* is obligated to maintain a secure online repository, which shall be available to all Relying Parties through a web interface at the following URL:

http://www.ca.ugrid.org/

It contains:

- the *UGRID CA* certificate for its signing key;
- all valid issued certificates referencing this Policy;
- the latest CRL;
- a copy of the current and of all previous versions of this CP/CPS document, under which certificates have been issued;
- the current list of the formally assigned staff members of the *UGRID CA*;
- the current list of the operational Registration Authorities;
- all available X.509 certificates of the staff members and RAs;
- all available PGP keys of the staff members, RAs, and the *UGRID CA* itself;
- official contact e-mail address and physical contact address of CA and RAs;
- other information related to certificates that refer to this Policy.

The repository is maintained on a best effort basis. Excluding maintenance shutdowns and unforeseen failures, the site should be available 24 hours a day, 7 days a week.

2.3 Time or frequency of publication

- Certificates will be published as soon as they are issued.
- CRL will be published immediately after it is updated following a revocation. It will be updated at least 7 days before the next update date of the CRL. The CRL life time is 30 days.
- This CP/CPS will be published whenever it is updated.

All other public information shall be published promptly after its update or after it becomes available to the CA.

2.4 Access control on repositories

The *UGRID CA* does not impose any access control restrictions on the information available at its online repository. However, the *UGRID CA* may to impose more restricted access control in future at its discretion.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Each subscriber must have a clear and unique Distinguished Name (DN) in the certificate subject field, structured according to the X.500 standards. The UGRID CA will ensure that a DN is not reused. If a person requests a certificate with the same DN as an existing certificate (regardless of the status of this certificate) and the request is not a renewal or rekey, the RA Operator will consult the original personal information to ensure that the Subscriber is the same as the person who was identified in the original certificate. If this identity cannot be established, the DN will never be reused.
The DN under this CP/CPS shall start with "DC=org, DC=ugrid". Thereafter, the subscriber's class, defined as either "*people*", "*hosts*", or "*services*", shall be attached in the form "O=*class*".
The DN may further contain the affiliation of the subscriber to his/her organization (this organization must be one of the organizational end-entities allowed for in section **1.3.3**) as organizationName attribute (O=). Inclusion of the affiliation is not entirely optional, but decided by the *UGRID CA*. If an organization consists of multiple administrative divisions, the division name may be included in the subject name as an organizationalUnitName attribute (OU=). Changes in the division name that do not change the organizational layout itself do not constitute reason to invalidate the current unit name.

In case of a **user** certificate, the commonName attribute (CN=) must include the full name of the subscriber in Latin letters as per his/her ID document. There must be at least two distinct (separated by spaces) parts in the name.
When the subscriber wishes to apply for multiple certificates with different DNs (e.g. for some of the Grid middleware), a serial number (left-padded with zeros to three digits, e.g. 003) or another appropriate set of distinguishing characters shall be added to the CN of each of the certificates.
If the subscriber wishes to include an e-mail address in the certificate, the address must not be part of the CN. Instead, it shall be included as rfc822Name attribute in the subjectAlternativeName extension.

In case of a **host** certificate, the commonName attribute (CN=) must include the fully-qualified domain name (FQDN) of the host. Additional FQDNs may be asserted in the subjectAlternativeName extension in multiple dNSName attributes. The FQDN must meet the PrintableString definition of RFC 2252, excluding comma, double quote, and single quote characters.

Otherwise (e.g. if the FQDN is an internationalized one), or if a FQDN is not assigned, the entity is not eligible for certification.

In case of a **service** certificate, the commonName attribute (CN=) must include the service name and the server's FQDN, separated by a forward slash. The service name and the FQDN must meet the PrintableString definition of RFC 2252, excluding comma, double quote, and single quote characters. Otherwise, or if an FQDN is not assigned, the entity is not eligible for certification.

3.1.2 Need for names to be meaningful

The subscriber must be represented by an easily understandable subject name associated with the authenticated name of the subscriber.

3.1.3 Anonymity or pseudonymity of subscribers

The *UGRID CA* shall not issue or sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

See section **3.1.1**.

3.1.5 Uniqueness of names

Global uniqueness of each subject name shall be guaranted by the *UGRID CA*. When this can not be achieved by other means, an appropriate set of distinguishing characters (e.g. a random number) shall be added to the commonName attribute.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of key

The *UGRID CA* verifies the possession of the private key of certificate requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to the requester. A cryptographic challenge-response exchange may be used to prove possession of the private key at any point in time before certification of the subscriber.
The *UGRID CA* shall not generate key pairs for the subscribers, nor shall it accept or retain private keys generated by the subscribers themselves.

3.2.2 Authentication of organization identity

Organizations shall be authenticated by the *UGRID CA* (or an RA on its behalf) on the basis of copies of signed and stamped official documents required by the Ukrainian law.

In order to ensure that the organization conforms to the requirements of section **1.3.3**., additional documents may be required.

3.2.3 Authentication of individual identity

Certificates, issued by the CA, bind a subject name to an identified entity that is in possession of the private key pertaining to that certificate. This binding shall be authenticated by the CA or its assigned RAs.
The initial authentication of natural person shall be based on government-issued identification documents and physical appearance of the applicant to the CA or RA.
If the entity is a machine or software component, the requester (a natural person) must provide proofs that the binding will be to the service or system defined in the subject and that the requester is adequately authorized.
When necessary, e-mail addresses shall be verified via non-cryptographic challenge-response technique.
The *UGRID* CA or RA will store photocopies of ID documents in case of user certificates and digitally signed e-mails in case of host or service certificates.

3.2.4 Non-verified subscriber information

During the initial identity validation the requester's e-mail is not verified, unless it will be present in the requested certificate.

3.2.5 Validation of Authority

The subscriber must present suitable documents proving any claimed affiliation with an organization.

3.2.6 Criteria of interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

To re-key before expiration one can send a re-key e-mail request, signed with the current user certificate. After expiration re-key procedure equals to the one for a new certificate. The subscriber must go through the procedure equal to the application for a new certificate at least once every 3 years.

3.3.2 Identification and authentication for re-key after revocation

A revoked key shall not be re-certified. Re-key after revocation follows the same authentication procedure as for a new certificate.

3.4 Identification and authentication for revocation request

The *UGRID CA* needs authentication of a revocation request, in case it cannot independently verify that the case is one of the listed in section **4.9.1**.
Certificate revocation requests should be submitted via e-mail. If made for a user certificate, the e-mail must be signed by the private key, corresponding to a non-expired, non-revoked valid certificate, issued by *UGRID CA* that is requested to be revoked. If it is made for a host or service certificate, the e-mail must be signed by the private key corresponding to a valid, non-expired, non-revoked the *UGRID CA* certificate of the person responsible for the given host or service. Revocation request by the RA should be done by e-mail, signed with valid RA operator key.
When using digitally signed e-mail is not an option, and in all cases not explicitly defined here, the authentication must be performed by the procedure for the initial identity validation (section **3.2**).

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

- The subject must be an acceptable subscriber as defined in section **1.3.3**;
- The applicant must have read and agreed to adhere to the policies and procedures described in this document;
- The applicant must generate a key pair using a trustworthy method, where the key length must be at least 1024 bits and the validity of the requested certificate must be at most one year plus one month. The *UGRID CA* will never generate a key pair for an applicant, nor will it accept private key escrow responsibilities. Requests that contain a private key shall be rejected immediately.
- The applicant must protect the private key with a secure pass phrase: at least 15 characters long and including small and capital letters, numerals, and punctuation signs. In case of a host or service certificate in automated environments where encryption of the private key is either impossible or does not constitute a benefit for the key security, the private key may be kept in unencrypted form. In any case, the physical and electronic access to the private key must be kept appropriately restricted at all times.

4.1.2 Enrollment process and responsibilities

The RA authenticates a subscriber for the first time and then once in 3 years, following the procedure described in section **3.2.3**.
After successful authentication, the subscriber must sign an explicit statement that he/she: *a*) has read this Policy and accepts to adhere to it; *b*) shall accept his/her certificate(s) signed by the *UGRID CA*; *c*) shall protect the relevant private key(s) in accordance with the rules of this Policy, and *d*) assumes the responsibility to notify the *UGRID CA* immediately in case of possible private key compromise or when a certificate is no longer required or when the information in a certificate becomes invalid.
Next, the RA shall assign a 25-character random code (capital letters and numerals, in groups of five, separated by dashes) to the request and supply it together with all the collected information (requester's name, e-mail address, affiliation, FQDN, service name, etc., as applicable) to the *UGRID CA* via a signed and encrypted e-mail, accompanied with a phone call to the relevant the *UGRID CA* staff member.
If the subscriber has opted to provide his certificate request directly to the RA in person at the time of authentication, the request shall also be included in the information supplied to the *UGRID CA*. Otherwise, the random code shall be provided to the subscriber, who has 5 working days from this point of time to submit his/her certificate request.

Unless the subscriber has provided his request for a new certificate directly to the RA in person, the submission of a request must be done either via encrypted e-mail to the RA before whom the subscriber has been authenticated or via an SSL protected web interface at the the *UGRID CA* online repository (section **2.2**).
When using e-mail, besides the request itself, it must also include the random code given at authentication. The e-mail must be encrypted to the relevant RA X.509 certificate or PGP key from the *UGRID CA* online repository.
The random code shall also be required when using the web interface.
If the subscriber wants to re-key his/her certificate, then he/she must follow the procedures described in section **4.7**.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

In the case of a new certificate, the request shall be authenticated and the information included within validated by the RA directly, as described in sections **3.2.2** and **3.2.3**. In the case of re-key of a valid, non-revoked, non-expired certificate, the authentication shall be performed by checking that the requester has a valid *UGRID CA* certificate (subject to the 3-year period described in section **4.1.2**).

4.2.2 Approval or rejection of certificate applications

To be approved the application request must conform to the following provisions:

- the certificate application must first be successfully authenticated;
- the subscriber must provide the correct random code during initial authentication or within 5 working days after a successful authentication performed by the RA;
- the subject must be an acceptable entity as defined by this Policy;
- the request must obey the *UGRID CA* distinguished name scheme;
- the distinguished name must be unambiguous and unique;
- the certificate key must have at least 1024 bits length.

If the certificate request does not meet one or more of the above criteria, it shall be rejected and a signed notification e-mail shall be sent to the applicant.

4.2.3 Time to process certificate applications

A certificate application shall take no more than 5 working days to be processed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Right after the subscriber's certificate has been issued, a signed and encrypted email shall be sent to the relevant RA, informing him/her about the action.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Right after the subscriber's certificate has been issued, a signed e-mail shall be sent to him/her with information on how to download his/her certificate from the *UGRID CA* online repository.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Since the subscriber has already declared that he/she will accept his/her certificate issued by the *UGRID CA* as described in section **4.1.2**, each certificate is considered accepted from the moment of its issuance.

4.4.2 Publication of the certificate by the CA

All certificates issued by the *UGRID CA* shall be published in the online repository as described in section **2**.

4.4.3 Notification of certificate issuance by the CA to other entities

Right after the subscriber's certificate has been issued, a signed and encrypted email shall be sent to the relevant RA, informing him/her about the action.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The issued by the *UGRID CA* certificates may be used for any application that is suitable for X.509 certificates (e.g. e-mail signing and encryption (S/MIME), authentication and encryption of communications (SSL/TLS), network layer encryption (IPsec), object-signing, etc.), explicitly excluding those described in section **1.4.2**. Subscriber’s keys must not be shared. The physical and electronic access to the private key must be kept appropriately restricted at all times. The subscriber must notify the *UGRID CA* immediately in case of possible private key compromise or when a certificate is no longer required or when the information in a certificate becomes invalid.

4.5.2 Relying party public key and certificate usage

The relying parties may use the certificates of the subscribers for the reciprocal activities of the stated ones in the previous section (e.g. signature verification, encryption). The relying parties should download the CRL at least once a day and implement its restrictions while validating certificates.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

The *UGRID CA* will not renew a subscriber's certificate. Subscribers must follow the re-key procedure as defined in section **4.7**.

4.6.2 Who may request renewal

Same as in section **4.6.1**.

4.6.3 Processing certificate renewal requests

Same as in section **4.6.1**.

4.6.4 Notification of new certificate issuance to subscriber

Same as in section **4.6.1**.

4.6.5 Conduct constituting acceptance of a renewal certificate

Same as in section **4.6.1**.

4.6.6 Publication of the renewal certificate by the CA

Same as in section **4.6.1**.

4.6.7 Notification of certificate issuance by the CA to other entities

Same as in section **4.6.1**.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Subscribers should regenerate their key pair in such cases:

- expiration of their certificate signed by the *UGRID CA.*

4.7.2 Who may request certification of a new public key

Same as in section **4.1.1**.

4.7.3 Processing certificate re-keying requests

The subscriber shall send a re-key request signed with the current user certificate before re-key expiration. The request must include the same explicit statement as the one signed by the subscriber after successful authentication, as described in **4.1.2**, where under "this Policy" the latest CP/CPS document, available from the *UGRID CA* online repository at this time, shall be assumed.
The *UGRID CA* reserves the right to reject the request or postpone its processing if the overlap between the new certificate and the old one would be unjustified.

Re-key after expiration or due to revocation or compromise of certificate must follow the same authentication procedure as the one described for a new certificate.
The subscriber must go through the procedure equal to the application for a new certificate at least once every 3 years.

4.7.4 Notification of new certificate issuance to subscriber

Same as in section **4.3.2**.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Since the subscriber has already declared that he/she will accept his/her certificate issued by the *UGRID CA* as described in section **4.7.3**, each re-keyed certificate is considered accepted from the moment of its issuance.

4.7.6 Publication of the re-keyed certificate by the CA

Same as in section **4.4.2**.

4.7.7 Notification of certificate issuance by the CA to other entities

Same as in section **4.4.3**.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A certificate should not be modified in any way.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate shall be revoked in any of the following cases:

- the subject of the certificate has ceased being eligible for certification as described in this Policy;
- the subject does not require the certificate any more;
- the private key has been lost or compromised;
- the information in the certificate is proven to be wrong or inaccurate;
- the host or service, to which the certificate had been issued, has been retired;
- the subscriber has failed to comply with the rules of this Policy.

4.9.2 Who can request revocation

The revocation of a certificate may be requested by:

- CA and RAs;
- the certificate subscriber him/herself;
- any other entity presenting proof of circumstance listed in section **4.9.1**.

4.9.3 Procedure for revocation request

The authentication of the entity requesting the certificate revocation shall be accomplished through signing the revocation request with a valid the *UGRID CA* certificate. If it is not available, the authentication must be performed within the procedure described in section **3.2.3**.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

The *UGRID CA* shall process all revocation requests in not more than one working day.

4.9.6 Revocation checking requirement for relying parties

Relying parties should download the CRL from the online repository (section **2.2**) at least once per day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency

CRL lifetime is 30 days. The CRL shall be issued immediately after each revocation, or at least 7 days before the expiration of the previous CRL.

4.9.8 Maximum latency for CRLs

The CRL shall be issued within one hour after each revocation.

4.9.9 On-line revocation/status checking availability
No stipulation.

4.9.10 On-line revocation checking requirements
No stipulation.

4.9.11 Other forms of revocation advertisements available
No stipulation.

4.9.12 Special requirements re key compromise
No stipulation.

4.9.13 Circumstances for suspension
The *UGRID CA* does not suspend certificates.

4.9.14 Who can request suspension
See section 4.9.13.

4.9.15 Procedure for suspension request
See section 4.9.13.

4.9.16 Limits on suspension period
See section 4.9.13.

4.10 Certificate status services

4.10.1 Operational characteristics
The *UGRID CA* online repository contains a CRL. Within one hour following revocation, the CRL and/or certificate database in the repository, as applicable, shall be updated.

4.10.2 Service availability
The online repository is maintained on a best effort basis with an intended availability of 24 hours a day, 7 days a week.

4.10.3 Optional features
No stipulation.

4.11 End of subscription
No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

The *UGRID CA* will not accept private key escrow responsibilities. Requests that contain a private key shall be rejected immediately.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The *UGRID CA* functions functions in a monitored area, located in the High-Performance Computing Center of the National Technical University of Ukraine "Kyiv Polytechnic Institute" where access is restricted. The *UGRID CA* signing machine and the repository web server are reserved exclusively for this purpose. The signing machine is not connected to any form of computer network.

5.1.2 Physical access

Physical access to The *UGRID CA* sites is restricted to the authorized personnel only, and the areas are under constant monitoring.

5.1.3 Power and air conditioning

The signing machine and the repository web server are both powered by a protected power supply. The environment temperature in the rooms containing the CA equipment is maintained at appropriate level by an air conditioning system and monitored by an independent mechanism.

5.1.4 Water exposures

Due to the location of the *UGRID CA* facilities, floods are not expected.

5.1.5 Fire prevention and protection

All facilities of the High-Performance Computing Center of the National Technical University of Ukraine "Kyiv Polytechnic Institute" adhere to the Ukrainian law regarding fire prevention and protection in public buildings.

5.1.6 Media storage

Backup copies of the *UGRID CA*-related information are kept in encrypted form on several removable storage media of different types (optical, magnetic, flash) in secure locations.

5.1.7 Waste disposal

Waste, containing potential confidential information, is physically destroyed before being dumped.

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural controls

5.2.1 Trusted roles

All employees, contractors, and consultants of the *UGRID CA* (collectively "personnel") that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

5.2.2 Number of persons required per task

No stipulation..

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The *UGRID CA* personnel must be familiar with the PKI infrastructure and operation, and possess the relevant technical and professional competence. There are no background checks or clearance procedures for trusted or other roles.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to the *UGRID CA* personnel.

5.3.4 Retraining frequency and requirements

The *UGRID CA* shall perform internal operational audit of the CA/RA staff at least once per year. If the results of the operational audit are not satisfactory, retraining and/or other appropriate measures shall be considered.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Documentation regarding all the operational procedures of the CA is supplied to the personnel during the initial training period.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Signing machine and repository server:

- system boots, reboots, and shutdowns
- user logins and privilege elevation ("su root")
- other important system information (e.g. kernel messages, etc.)

In general:

- requests for certificate (including log when request comes and when it is approved or deleted)
- requests for revocation
- certificate issuing
- CRL issuing

5.4.2 Frequency of processing log

Audit logs shall be processed at least once per month.

5.4.3 Retention period for audit log

Audit logs shall be retained for a minimum of 3 years after all certificates, relevant to these logs, have expired.

5.4.4 Protection of audit log

Only authorized the *UGRID CA* personnel is allowed to access and process audit logs. The audit logs never leave the *UGRID CA* site of operation, except (for the electronic logs) in encrypted form for backup purposes as stated in next section.
The electronic audit logs are protected by UNIX-style file system permissions.
The paper audit logs are kept in a locked strongbox.

5.4.5 Audit log backup procedures

The electronic audit logs are regularly (at least once per month) copied to an off-line medium, which is stored in a location with the same access restrictions as for the

UGRID CA site of operation. Prior to copying, the audit logs shall be encrypted with a suitable secure mechanism.

5.4.6 Audit collection system (internal vs. external)

The audit log accumulation system is internal to the *UGRID CA.*

5.4.7 Notification to event-causing subject

Entities that cause an audit event are not explicitly notified of the audit action.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

- all certificate and revocation requests;
- all issued certificates and CRLs;
- all data (either on paper or in electronic form), pertaining to the identity verification and certificate request information validation;
- all electronic and paper correspondence of the CA;
- periodic digests of important system log files of the issuing machine and the repository server;
- all signed agreements with other parties.

5.5.2 Retention period for archive

The archive shall be kept for a minimum of 3 years after all certificates, relevant to the archived records, have expired.

5.5.3 Protection of archive

Only authorized *UGRID CA* personnel is allowed access to the record archives. The archives never leave the *UGRID CA* premises, except (for the electronic documents) in encrypted form for backup purposes as stated in next section. The electronic data are protected by UNIX-style file system permissions. The paper documents are kept in a locked strongbox.

5.5.4 Archive backup procedures

The electronic record archives are regularly (at least once per month) copied to an off-line medium, which is stored in a location with the same access restrictions as for The *UGRID CA* site. Prior to copying, the record archives shall be encrypted with a suitable secure mechanism.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to the *UGRID CA*.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The *UGRID CA* will generate a new key pair when its current root certificate is due to expire. From the moment the new CA root certificate is published online only the new private key shall be used for certificate signing purposes. The old but still valid root certificate shall be available to verify old signatures, and the old private key shall be available to sign relevant CRLs, until all the certificates signed using that key have expired or been revoked. The overlap between the old and the new key shall be at least one year plus one month.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

If the *UGRID CA* private key is compromised or suspected to be compromised, or if it is destroyed, the *UGRID CA* shall immediately:

- notify the subscribers and the RAs, as well as the relevant relying parties of which/whom the *UGRID CA* is aware;
- terminate the issuance and distribution of certificates and CRLs until a new key pair is generated and the new CA root certificate is published online;
- notify all other relevant security contacts.

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

The private keys of the *UGRID CA* are only available in encrypted form on media stored in a secure location. The machine used to activate the private key is not accessible via any network. If the machine and/or the media are lost, this shall be handled as a major compromise that implies generating a new key pair and terminating all services associated with the lost key pair.

If the hardware or software of the signing machine becomes corrupt, the status shall be diagnosed and suitably repaired. If there is any doubt about the extent of the damage involved, this shall imply rebuilding the machine from scratch, using original supplied parts and software distributions.

If data become corrupted, the cause shall be diagnosed and the data should be restored from the latest back-up.

5.7.3 Entity private key compromise procedures

If an entity's private key is compromised or suspected to be compromised, or if it is destroyed, the subscriber must immediately request revocation of the certificate and inform all relevant relying parties.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

Upon permanent termination of its activities as a CA, the *UGRID CA* shall:

- notify the subscribers and the RAs, as well as the relevant relying parties of which/whom the *UGRID CA* is aware;
- terminate the issuance and distribution of certificates and CRLs;
- notify all relevant security contacts;
- make the information of its termination as public as possible.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs for the CA, RAs, and subscribers must be generated in such a way that the private key is not known by any other than the owner of the key pair.
Key pairs for the *UGRID CA* are generated exclusively by authorized the *UGRID CA* staff members on a dedicated, disconnected from all computer networks system, using a recent, trustworthy version of the OpenSSL software package on a UNIX or UNIX-like operating system.
The *UGRID CA* does not generate private keys on behalf of subscribers. The subscribers' private keys must never be sent to the *UGRID CA.*

6.1.2 Private key delivery to subscriber

Not applicable (see previous section).

6.1.3 Public key delivery to certificate issuer

The subscriber's public key must be transferred to the *UGRID CA* in a secure way (either via encrypted e-mail or via an SSL protected web interface).

6.1.4 CA public key delivery to relying parties

The *UGRID CA* root certificate is available for download from the online repository (section **2.2**).

6.1.5 Key sizes

The minimum key length for a person, host, or service certificate is 1024 bits.
The minimum length for the *UGRID CA* signing key is 2048 bits.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

The *UGRID CA* root certificate shall have:

- the basicConstraints extension marked critical and set to "CA:true";
- the keyUsage extension marked critical, with the keyCertSign and cRLSign bits set.

End entity certificates issued by the *UGRID CA* under this Policy shall have:

- the basicConstraints extension marked critical and set to "cA:false";
- the keyUsage extension marked critical, with digitalSignature and keyEncipherment bits set; other bits may be set as well if required, except for

nonRepudiation in host and service certificates, and keyCertSign and cRLSign in all certificates;
- the extendedKeyUsage including clientAuth/serverAuth KeyPurposeId; other KeyPurposeIds (emailProtection, codeSigning, etc.) may be included as well if required.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The *UGRID CA* private key is kept in encrypted form on media storage as described in section **5.1.6**. All media are located in secure places, where access is restricted to authorized personnel only. Paper copy of the private key's pass phrase is also kept in a secure place.

6.2.5 Private key archival

The *UGRID CA* does not archive private keys except its own private key corresponding to the UGRID CA certificate.

6.2.6 Private key transfer into or from a cryptographic module

The *UGRID CA* does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

The *UGRID CA* does not use any kind of cryptographic module.

6.2.8 Method of activating private key

The private key of the *UGRID CA* is activated by using a pass phrase. See section **6.4.1**

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

After termination of the CA, all media that contain the private key of the CA shall be securely and permanently destroyed, according to the best practice at that time.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

All certificates issued to subscribers by the *UGRID CA* shall have a maximum lifetime of one year plus one month. The lifetime of the *UGRID CA* root certificate is 5 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The pass phrase used to activate the *UGRID CA* private key is generated on the computer used for the CA signing operations. It must be at least 15 characters long and include small and capital letters, numerals, and punctuation signs. The pass phrase shall be changed at irregular intervals of time, at least two times per year.
The *UGRID CA* does not generate activation data for subscribers. It is upon the subscriber to generate a secure pass phrase, at least 15 characters long, and including small and capital letters, numerals, and punctuation signs, in order to be used as activation data for his/her private key.

6.4.2 Activation data protection

The pass phrase for the *UGRID CA* signing key is known only to the authorized the *UGRID CA* operators. A copy of the pass phrase in written form, for backup purposes, is kept in sealed envelope in a locked strongbox. Access to the strongbox is restricted only to the authorized personnel. The envelope is checked for tampering at least once a week. Old activation data are destroyed according to the best practices at that time.
For end entity certificates, the subscriber is responsible for protecting the activation data for the private key.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

- The operating systems of CA/RA computers are maintained at a high level of security by applying all necessary patches and updates in a timely manner.
- Proactive monitoring is performed to detect unauthorized software changes.
- CA systems configuration is kept at the bare minimum.
- The signing machine is kept disconnected from all computer networks at any time. Any required patches and updates are downloaded on the online repository server, and are strictly verified for correctness, if applicable (e.g. MD5/SHA256 hashes, PGP signatures). Whenever available, source code versions are preferred before the binary ones.
- The signing machine is kept powered down between uses.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

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 *UGRID CA* signing machine is kept disconnected from all computer networks at any time.
- CA/RA machines other than the signing machine are protected by highly restrictive firewalls.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All certificates under this Policy shall be issued in the X.509 version 3 format and shall include a reference to the OID of this Policy within the appropriate field.

7.1.2 CA Certificate extensions

- *basicConstraints* [critical] CA: true
- *keyUsage* [critical] keyCertSign, cRLSign
- *subjectKeyIdentifier* hash
- *authorityKeyIdentifier* keyIdentifier

7.1.3 Certificate extensions

- *basicConstraints* [critical] CA: false
- *keyUsage* [critical] digitalSignature, keyEncipherment

Other bits may be set as well if required, except for nonRepudiation in host and service certificates, and keyCertSign and cRLSign in all certificates.

- *extendedKeyUsage* clientAuth

Other KeyPurposeIds (emailProtection, codeSigning, etc.) may be included as well if required.

- *crlDistributionPoints* at least one http URL
- *authorityKeyIdentifier* keyIdentifier
- *subjectKeyIdentifier* hash
- *certificatePolicies* OID specified in section **1.2**
- *subjectAlternativeName, issuerAlternativeName* dNSName or rfc822Name

subjectAlternativeName shall be present for host and service certificates and shall contain at least one FQDN in the dNSName attribute. rfc822Name attribute shall be used when an end entity certificate needs to contain an RFC 822 email address.
Other certificate extensions may be added when needed and appropriate.

7.1.4 Algorithm object identifiers

The UGRID CA uses SHA1 with RSA encryption as its signature algorithm.

7.1.5 Name forms

The distinguished name of the CA is “DC=org, DC=ugrid, CN=UGRID CA”. See section **3.1.1** for the name forms of subscriber certificates.

7.1.6 Name constraints
See section **3.1.1**.

7.1.7 Certificate policy object identifier
The UGRID CA identifies this Policy with the object identifier specified in section **1.2**.

7.1.8 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)
All CRLs shall be issued in X.509 version 2 format.

7.2.2 CRL and CRL entry extensions
No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)
No stipulation.

7.3.2 OCSP extensions
No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The *UGRID CA* may be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document. Any costs associated with such an audit must be covered by the requesting party.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

No stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees shall be charged.

9.1.2 Certificate access fees

No fees shall be charged.

9.1.3 Revocation or status information access fees

No fees shall be charged.

9.1.4 Fees for other services

No fees shall be charged.

9.1.5 Refund policy

Not applicable (see sections **9.1.1** – **9.1.4**).

9.2 Financial responsibility

The *UGRID CA* denies any financial responsibilities for damages or impairments resulting from its operation.

9.2.1 Insurance coverage

Not applicable (see section **9.2**).

9.2.2 Other assets

Not applicable (see section **9.2**).

9.2.3 Insurance or warranty coverage for end-entities

Not applicable (see section **9.2**).

9.3 Confidentiality of business information

The *UGRID CA* does not collect any confidential business information.

9.3.1 Scope of confidential information

Not applicable (see section **9.3**).

9.3.2 Information not within the scope of confidential information

Not applicable (see section **9.3**).

9.3.3 Responsibility to protect confidential information

Not applicable (see section **9.3**).

9.4 Privacy of personal information

The UGRID CA does not collect any confidential or private information except for the case when the UGRID CA or RA stores photocopies of ID documents to perform identitiy validation for a user certificate request. The UGRID CA and RA guarantee that this information is not used for any other purposes.

9.4.1 Privacy plan

Not applicable (see section **9.4**).

9.4.2 Information treated as private

Not applicable (see section **9.4**).

9.4.3 Information not deemed private

The *UGRID CA* collects the following information which is not deemed as private:

- subscriber's e-mail address;
- subscriber's name;
- subscriber's organization;
- subscriber's certificate.

9.4.4 Responsibility to protect private information

Not applicable (see section **9.4**).

9.4.5 Notice and consent to use private information

Not applicable (see section **9.4**).

9.4.6 Disclosure pursuant to judicial or administrative process

Not applicable (see section **9.4**).

9.4.7 Other information disclosure circumstances

Not applicable (see section **9.4**).

9.5 Intellectual property rights

IETF RFC 3647
Bulgaria CA Certification Authority Certificate Policy and Certificate Practice Statement
Romania, ROSA CA Certificate Policy and Certificate Practice Statement
AEGIS Certificate Policy and Certificate Practice Statement
CERN Certification Authority Certificate Policy and Certification Practice Statement

BalticGrid CA Certificate Policy and Certification Practice Statement
SWITCH Certificate Policy and Certification Practice Statement
UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
The DutchGrid Science Certification Authority Certificate Policy and Certification Practices Statement

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

- The *UGRID CA* guarantees to control the identity of the certification requests according to the procedures described in this document
- The *UGRID CA* guarantees to control the identity of the revocation requests according to the procedures described in this document
- The *UGRID CA* is run on a best effort basis and does not give any guarantees about the service security or suitability
- The *UGRID CA* shall not be held liable for any problems arising from its operation or improper use of the issued certificates
- The *UGRID CA* denies any kind of responsibilities for damages or impairments resulting from its operation

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.