Belarusian Grid Certification Authority

Certificate Policy and

Certification Practice Statement

Version 1.1

Document OID: 1.3.6.1.4.1.24432.11.1.1.1

07 October 2008

Contents

1 INTRODUCTION

This document describes the rules and procedures used by the Belarusian Grid Certification Authority operated by the United Institute of Informatics Problems of the National Academy of Sciences of Belarus.

1.1 Overview

The State scientific organization "United Institute of Informatics Problems of the National Academy of Sciences of Belarus" (UIIP NASB) is the leading Belarusian institution for carrying out fundamental and applied research in the fields of information technology and computer science. The UIIP NASB's staff is more than 400 persons including 264 research workers. Presently the UIIP NASB takes active part in two grid projects:

  – Development of Grid Technologies and New Generation SKIF-Supercomputers (SKIF-Grid);

  – Baltic Grid Second Phase (BalticGrid-II).

Additional information about the UIIP NASB can be obtained at http://uiip.bas-net.by.

In order to strengthen Belarusian grid infrastructure and facilitate its efficient usage by national research community, as well as to allow full integration of Belarusian user community and computing resources into the BalticGrid, the pan-European and other Grid infrastructures, it was necessary to establish the Belarusian Grid Certification Authority (BYGCA).

The BYGCA will provide security infrastructure needed for the operation of all of Belarusian grid resources and authentication of all Belarusian grid users, hosts and services.

The UIIP NASB will manage, coordinate and further develop the BYGCA.

This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the BYGCA in issuing certificates as well as the responsibilities of the involved parties.

The BYGCA is operated at the premises of the UIIP NASB located in the main building of the UIIP NASB.

This document is structured according to RFC 3647.

This document was issued on 07 October 2008, and took effect on 10 October 2008.

1.2 Document name and identification

1. Document title: "Belarusian Grid Certification Authority Certificate Policy and Certification Practice Statement".

2. Document version: 1.1.

3. Document date: 07 October 2008.

4. Effective from: 10 October 2008.

5. ASN.1 Object Identifier (OID): 1.3.6.1.4.1.24432.11.1.1.1.

The next table describes the meaning of the OID:

1.3.6.1.4.1	Prefix for IANA private enterprises
.24432	UIIP NASB
.11	BYGCA
.1	CP/CPS
.1.1	Major and minor CP/CPS number

1.3 PKI participants

1.3.1 Certification Authorities

The BYGCA is defined as a medium security certification authority (CA). The BYGCA does not issue certificates to subordinate certification authorities.

1.3.2 Registration authorities

The BYGCA manages the functions of its Registration Authority (RA). The RA Operators are responsible for verifying subscribers' identities and approving their certificate requests. RA Operators do not issue certificates. The list of RAs is available on the BYGCA's website: http://ca.grid.by.

Each RA MUST sign an agreement with the BYGCA, stating their adherence to the procedures described in this CP/CPS.

1.3.3 Subscribers

The BYGCA issues personal (user), host and service certificates. Subscribers eligible for certification from the BYGCA are all those related to organizations, formally based in and/or having offices in Belarus, that are involved in research or deployment of multidomain distributed computing infrastructure, intended for cross-organizational sharing of resources.

1.3.4. Relying parties

Users of grid computing infrastructures that are using the public keys in certificates issued by the BYGCA 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 uses

Personal (user) certificates can be used to authenticate a user that would like to benefit from the grid resources.

Host certificates can be used to identify computers that have special tasks related to the grid activities.

Service certificates can be used to recognize the host applications and data or communication encryption (SSL/TLS).

In addition, it is permissible to use personal certificates for email signing and user authentication using HTTP Secure protocol.

1.4.2 Prohibited certificate uses

Notwithstanding the above, using certificates for purposes contrary to the law in the Republic of Belarus is explicitly prohibited.

1.5 Policy administration

1.5.1 Organization administering the document.

The BYGCA CP/CPS document was authored and is administered by the United Institute of Informatics Problems of the National Academy of Sciences of Belarus – the UIIP NASB.

The BYGCA address for operations issues is:

Belarusian Grid Certification Authority
United Institute of Informatics Problems of the National Academy of Sciences of Belarus
Surganova St., 6
Minsk 220012, Belarus
Tel.: +375 29 2842083
e-mail: ca@newman.bas-net.by

1.5.2 Contact person

Contact person for questions related to this document or any other BYGCA related issue is:

Yury Ziamtsou
United Institute of Informatics Problems of the National Academy of Sciences of Belarus
Surganova St., 6
Minsk 220012, Belarus
Tel.: +375 29 2842083
e-mail: ca@newman.bas-net.by

1.5.3 Person determining CPS suitability for the policy

The person who determines the CPS suitability for the policy is the same person as in section 1.5.2.

1.5.4 CPS approval procedures

New versions of the Certification Practice Statement are reviewed internally in order to verify their suitability against the minimum requirements, which are defined by the IGTF. Internal approval is followed by the submission of major changes (if any) of the CP/CPS to the EUGridPMA, in order to be approved. The minor changes are announced to the EUGridPMA.

1.6 Definitions and acronyms

ASN.1	Abstract Syntax Notation One
BYGCA	Belarusian Grid Certification Authority
CA	Certification Authority
CN	Common Name
CP/CPS	Certificate Policy/Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DNS	Domain Name System
EUGridPMA	European Policy Management Authority for Grid Authentication
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IGTF	International Grid Trust Federation
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
O	Organization
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Change
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UIIP NASB	United Institute of Informatics Problems of the National Academy of Sciences of Belarus
URL	Uniform Resource Locator
USB	Universal Serial Bus

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The BYGCA operates an on-line repository that contains:

- the BYGCA root certificate;
- Certificate Revocation Lists (periodically updated);
- a copy of the most recent version of this CP/CPS and all previous versions;
- a list of current operational Registration Authorities;
- links to all trust anchor repositories where BYGCA info is published;
- other relevant information.

The BYGCA communication information for information regarding repositories is:

Belarusian Grid Certification Authority
United Institute of Informatics Problems of the National Academy of Sciences of Belarus
Surganova St., 6
Minsk 220012, Belarus
Tel.: +375 29 2842083
e-mail: ca@newman.bas-net.by
Web: http://ca.grid.by

2.2 Publication of certification information

The BYGCA is obliged to maintain on-line repository which is described in section 2.1.

2.3 Time or frequency of publication

Certificates will be published as soon as they are issued.

CRL publication frequency is defined in section 4.9.7.

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

2.4 Access control on repositories

The online repository is maintained on best effort basis and is available substantially on a 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance. The BYGCA may impose a more restricted access control policy to the repository at its discretion. The BYGCA does not impose any access control on its CP/CPS, issued certificates or CRLs.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Any name under this CP/CPS starts with "DC=by, DC=grid".

The subject names should be formatted as per X.501 standard. All parts of the name are encoded as PrintableStrings.

1. In case of root certificate:
   - Common Name must be "Belarusian Grid Certification Authority".
   - Organization must be "uiip.bas-net.by".

2. In case of personal certificate:
   - Common Name must include the person's first name and last name.
   - Organization must include the organization domain name.

3. In case of host certificate:
   - Common Name must be the host DNS name (FQDN).
   - Organization must include the organization domain name.

4. In case of grid service certificate:
   - Common Name must include the "servicename/" prefix, followed by the host DNS name (FQDN).
   - Organization must include the organization domain name.

3.1.2 Need for names to be meaningful

The subject's and issuer's names contained in a certificate must be meaningful in the sense that the BYGCA has proper evidence of the existent association between these names and the entities to which they belong.

For personal certificates, the Common Name attribute contains the legal name in English alphabet as presented in a passport of a resident of the Republic of Belarus. The CN of a personal certificate may contain additional text other than the subscriber's authenticated name, in order to disambiguate between different users with the same name, or to allow the same user to have more than one certificate. The additional text must be formatted in such as way so as not to be confused with the subscriber's name; it is recommended that it follows the subscriber's name, with a space as separator, and enclosed in parentheses. The CA does not otherwise enforce or validate the content of this text, and relying parties are explicitly forbidden to rely on the content of this additional text, or attribute any semantic value to it, for any authentication or authorization purposes.

For host certificates, the CN attribute contains the fully qualified domain name of the server.

For grid service certificates, the CN must be related to the type of service the certificate is identifying.

3.1.3 Anonymity or pseudonimity of subscribers

The BYGCA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

See section 3.1.1 and Section 3.1.2.

3.1.5 Uniqueness of names

Distinguished names for each certificate must be unambiguous and unique, and it must be linked to one and only one entity over the entire lifetime of the BYGCA. When essential, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name. Single subscriber may have more than one associated distinguished name.

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 BYGCA proves possession of the private key that is the companion to the BYGCA root certificate by issuing certificates and signing CRLs. The BYGCA verifies the possession of the private key relating to certificates 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 requester. A cryptographic challenge-response exchange may be used to prove possession of the private key at any point in time before certification of subscriber.

The BYGCA will not generate the key pair for subscribers and will not accept or retain private keys generated by subscribers.

3.2.2 Authentication of organization identity

RA must verify the authentication of organization by checking if:

1. The organization is known to be part of a grid-computing project or related partner.

2. The organization is registered and operates in the Republic of Belarus. Registration will be validated through proper public authorities.

The person who issues a request must demonstrate the relation between him/her and the organization he/she represents.

3.2.3 Authentication of individual entity

1. Certificate of a person:

The subject should personally meet the RA staff in order to validate his/her identity. Authentication of the subject is fulfilled by providing a passport of a resident of the Republic of Belarus declaring that the subject is a valid end entity. Subject's affiliation must be proven by specific ID document issued by subject's organization. Upon authentication of the subjects the RA will make a photocopy of the ID documents. The gathered photocopies will be forwarded to the CA for archival.

2. Certificate of a host or service:

Host certificates can only be requested by the administrator responsible for the particular host. The certificate requests are sent to RA by e-mail signed by the responsible administrator. In order to request a host certificate the following conditions must be met:

1. The host must have a valid FQDN.

2. The administrator must already possess a valid personal BYGCA certificate.

3. The administrator must provide a proof of his or hers relation to the host itself. It can be done by having himself or herself declared as an administrator of the specific host at the website identified with the FQDN of that host.

The RA must archive all email requests for the approved host or service certificate requests.

3.2.4 Non-verified subscriber information

During the initial identity validation the requester's e-mail is not verified. This is done during the processing of the certificate application as described in section 4.2.2.

3.2.5 Validation of Authority

The subscriber requesting service from the BYGCA must present valid documents stating his/her affiliation with the 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

Expiration warnings will be sent to subscribers before it is re-key time. Re-key before expiration can be executed by stating a re-key request signed with the private key corresponding to a valid certificate of the subscriber. Re-key after expiration uses completely the same authentication procedure as new certificate. Once every 3 years the subscriber has to be authenticated by the local RA as described in 3.2.3.

3.3.2 Identification and authentication for re-key after revocation

The procedure for re-authentication is exactly the same with an initial registration.

3.4 Identification and authentication for revocation request

Certificate revocation requests should be authenticated in one of the following ways:

– By signing a revocation request e-mail with the private key corresponding to the certificate that is requested to be revoked which must be a valid, non-expired and non-revoked certificate issued by the BYGCA.

– For persons who do not have a valid BYGCA certificate, but hold an evidence of a revocation circumstance: by personal authentication as described in 3.2.3.

– If the revocation request is for a host or service certificate, then the e-mail must be signed by the private key corresponding to the certificate of the person responsible of the host or service. When e-mail is not an option, the request will be authenticated using the procedure described in section 3.2.3.

– Revocation request from RA should be done by e-mail signed with a valid RA operator key.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

The applicant must:

1. be an acceptable subscriber as stated in section 1.3.3;

2. read and adhere to all of the statements of this document;

3. generate a key-pair using a trustworthy method. The private key must be 1024 or 2048 bits;

4. use a strong passphrase.

4.1.2 Enrollment process and responsibilities

1. User certificate:

A subscriber must submit the certificate requests via e-mail to the serving RA. A subscriber must be authenticated by the RA serving his/her location following the procedure described in section 3.2.3. If the subscriber wants to re-key his/her certificate, then he/she must follow the procedures described in section 4.7.

2. Host or service certificate:

The subject must already have a valid user certificate issued by the BYGCA before requesting a host or service certificate. The submission of the certificate request can be done via e-mail. The subject will have to send an e-mail signed with his/her private key

corresponding to a valid user certificate issued by the BYGCA to e-mail from section 1.5.1 with the certificate requests attached and stating in the body of the e-mail that he is the person responsible for the host/service. The certificate request will be forwarded to the appropriate RA, who will approve or disapprove the request according to sections 4.2.1 and 4.2.2

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All the certificate applications will be authenticated and validated by the BYGCA RAs as stated in section 3.2.3. A case of re-key is addressed in section 3.3.1. Upon successful authentication, the information included in the certificate request will be validated by CA.

4.2.2 Approval or rejection of certificate applications

The essential procedures that must be conformed in a certificate application request are as follows:

1. the subscriber must be authenticated by RA;

2. the subject must be an acceptable subscriber entity, as defined by this Policy;

3. the subject must have a valid e-mail address;

4. the request must obey the BYGCA distinguished name scheme;

5. the distinguished name must be unique;

6. the key must be 1024 or 2048 bits;

7. applicant generates his/her own key;

8. host and service certificate requests must be submitted via e-mail signed by the private key corresponding to a valid user certificate issued by the BYGCA;

9. requests for certification keys with exponent equal to 3 will be rejected.

If the certificate request does not meet one or more of the above criteria, it will be rejected and signed notification e-mail will be sent by the RA to the subject with carbon copy to the e-mail address from section 1.5.1.

4.2.3 Time to process certificate applications

Each certificate application will take no more that 5 working days to be processed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After CA receives certificate request the request is transferred to the dedicated CA machine by using removable media. Certificate is signed and transferred back to the web repository by using removable media. After the subscriber's certificate is issued, an e-mail

will be sent to the relevant RA manager and to the subscriber itself informing him/her about the action.

4.3.2 Notification to subscriber by the CA of issuance of certificate

If the subscriber has requested a certificate through the RA, an e-mail will be sent to the relevant RA manager right after subscriber's certificate is issued.

4.4 Certificate acceptance

The certificate is assumed to be accepted unless its requester explicitly rejects it in an authenticated communication with the CA.

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

Corresponding RA that has handled the communication with the requesting subscriber will be notified of the certificate issuance. The RA will be informed about any certificate signatures and re-keys before expiration that were submitted through it.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscribers' private key along with the certificates issued by the BYGCA usage is defined in section 1.4.1. The private key associated with any certificate must not be disclosed to or shared with end-entities other than the one to which the certificate was issued.

4.5.2 Relying party public key and certificate usage

Relying parties can use the public keys and certificates of the subscribers for:

1. E-mail encryption and signature verification (S/MIME);

2. Host authentication and encryption of communications;

3. User authentication. Relying parties must 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 BYGCA will not renew subscribers' certificates. 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 Circumstances for certificate re-key

Subscribers must regenerate their key pair in the following circumstances:
1. expiration of their certificate signed by the BYGCA;
2. revocation of their certificate by the BYGCA;

Subscribers can regenerate their key pair 30 days before certificate expiration.

4.7.2 Who may request certification of a new public key

Same as in section 4.1.1, under the circumstances given in 4.7.1.

4.7.3 Processing certificate re-keying requests

Expiration warnings will be sent to subscribers before it is re-key time. Re-key before expiration can be executed by stating a re-key request signed with the private key corresponding to a valid user certificate of the subscriber. Re-key after expiration uses completely the same authentication procedure as new certificate. As mentioned in section 3.3.1 once in the specified period the subscriber must go through the same authentication procedure. In case the request for a new certificate is due to revocation or compromise of certificate the subscriber must follow the same procedure as the one described in for a new one.

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

Same as in section 4.4.1.

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 Circumstances for certificate modification

The BYGCA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.2 Who may request certificate modification

Same as in section 4.8.1.

4.8.3 Processing certificate modification requests

Same as in section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

Same as in section 4.8.1.

4.8.5 Conduct constituting acceptance of modified certificate

Same as in section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

Same as in section 4.8.1.

4.8.7 Notification of certificate issuance by the CA to other entities

Same as in section 4.8.1.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate will be revoked when the information it contains or the implied assertions it carries are known or suspected to be incorrect, compromised or the subscriber does not need the certificate any more. This includes situations where:

– the BYGCA is informed that the subscriber has ceased to be a member of or associated with any grid program or activity;

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

– the information in the subscriber's certificate is wrong or inaccurate, or suspected to be wrong or inaccurate;

– the subscriber violates his/her obligations;

– the subscriber does not need the certificate any more;

– evidence presented from any other entity of revocation circumstances.

4.9.2 Who can request revocation

The BYGCA, its RA, the subscriber of the certificate or any other entity holding evidence of a revocation circumstance about that certificate can request revocation.

4.9.3 Procedure for revocation request

The entity requesting the certificate revocation is authenticated by signing the revocation request with the private key corresponding to a valid user certificate issued by the BYGCA. Otherwise authentication will be performed with the same procedure as described in section 3.2.3. Also if the BYGCA or its RA can individually prove by performing individual analysis that evidence for revocation provided by third party is correct it will be accepted as valid request.

4.9.4 Revocation request grace period

The BYGCA has a maximum response time of one day (excluding weekends and public holidays of the Republic of Belarus) for revocations; it will however handle revocation requests with priority as soon as the request is recognized as such.

4.9.5 Time within which CA must process the revocation request

The BYGCA will process all revocation requests within one day (excluding weekends and public holidays of the Republic of Belarus) after receiving a revocation request.

4.9.6 Revocation checking requirement for relying parties

Relying parties must download the CRL from the online-repository [section 2.2] at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency

1. CRLs will be published in the on-line repository as soon as issued and at least once every 30 days;

2. The minimum CRL lifetime is 7 days;

3. CRLs are issued at least 7 days before expiration.

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

Currently there are no on-line revocation/status services offered by the BYGCA.

4.9.10 On-line revocation checking requirements

Same as in section 4.9.9.

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 BYGCA does not suspend certificates.

4.9.14 Who can request suspension

Same as in section 4.9.13.

4.9.15 Procedure for suspension request

Same as in section 4.9.13.

4.9.16 Limits on suspension period

Same as in section 4.9.13.

4.10 Certificate status services

4.10.1 Operational characteristics

The BYGCA operates an on-line repository that contains all the CRLs that has been issued. Promptly following revocation, the CRL or certificate status database in the repository, as applicable, shall be updated.

4.10.2 Service availability

The on-line repository is maintained on best effort basis with intended availability of 24x7.

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 BYGCA will not accept any key escrow or recovery services and will not give keys on escrow as well.

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 BYGCA operates in a controlled and protected room located in the UIIP NASB. At least one person employed by the UIIP NASB always will be present on premises 24 hours per day, 7 days per week.

5.1.2 Physical access

Physical access to the BYGCA is restricted to authorized personnel only.

5.1.3 Power and Air Conditioning

Premises containing the BYGCA machine are air conditioned.

5.1.4 Water Exposures

Due to the location of the BYGCA facilities floods are not expected. The BYGCA secure operating room is reasonably waterproof; no water exposure is expected to occur.

5.1.5 Fire Prevention and Protection

Buildings containing the BYGCA facilities obey to the Belarusian laws regarding fire prevention and protection of buildings.

5.1.6 Media storage

Backups are to be stored in removable storage media.

The BYGCA key is kept in several removable storage media.

Backup copies of CA related information are kept in USB storage devices and on CD-ROMs.

5.1.7 Waste Disposal

Removable storage media are physically destroyed before being trashed.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

No stipulation.

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 BYGCA personnel are recruited from the grid team of the UIIP NASB. They are familiar with the importance of a PKI, technically and professionally competent.

Registration Authorities personnel is recruited from personnel of corresponding institutions.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to the BYGCA and RA operators.

5.3.4 Retraining frequency and requirements

No stipulation.

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 BYGCA is supplied to personnel during the initial training period.

5.4 Audit logging procedures

5.4.1 Types of events recorded

CA must keep log of the following events:

- certification requests;

- issued certificates;

- requests for revocation;

- issued CRLs;

- login/logout/reboot of the signing machine;

Each RA must keep log of the following:

- for each approved request, how it was approved;

- for each rejected request, why it was rejected;

- for each approved revocation request, the reason for revocation;

- for each rejected revocation request, the reason for revocation and the reason the request was rejected.

5.4.2 Frequency of processing log

Audit logs will be processed at least once per quarter.

5.4.3 Retention period for audit log

Audit logs will be retained for a minimum of 3 years.

5.4.4 Protection of audit log

Only authorized BYGCA personnel are allowed to view and process audit logs. Audit logs are kept in a safe storage in a room with limited access.

5.4.5 Audit log backup procedures

Audit logs are copied to an offline medium and kept in a safe storage in a room with limited access.

5.4.6 Audit collection system (internal vs. external)

Audit log collection system is internal to the BYGCA.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The following data and files are recorded and archived by the BYGCA:

- certification requests;
- issued certificates;
- requests for revocation;
- issued CRLs;
- all e-mail messages of correspondence between the RA and the BYGCA;
- login/logoff/reboot of the signing machine;
- personal identification photocopies gathered by the RA.

The BYGCA recorded events will be logged on paper and archived by the BYGCA and kept in a safe in the BYGCA premises.

Each RA must archive log of the following events:

- for each approved request, how it was approved;
- for each rejected request, why it was rejected;
- for each approved revocation request, the reason for revocation;
- for each rejected revocation request, the reason for revocation and the reason the request was rejected.

The RA recorded events will be logged in electronic form and kept in premises of the RA with controlled access.

5.5.2 Retention Period for Archive

Minimum retention period is three years.

5.5.3 Protection of Archive

Archives are kept in a safe storage in a room with limited access.

5.5.4 Archive backup procedures

All data and files are copied to an off-line medium.

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 BYGCA.

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Key changeover

The BYGCA private key is changed periodically; from that time on, the new key will be valid in order to sign new certificates or CRL lists of new certificates. The overlap of the old and new key must be at least maximum validity period for certificates as defined in section 6.3.2. The older but still valid certificate must be available to verify old signatures and its private key must be used to sign CRLs until all the certificates signed using the associated key have expired or been revoked.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

If the BYGCA private key is (or is suspected to be) compromised, the BYGCA will:

- inform the EUgridPMA;

- inform the Registration Authorities, subscribers and relying parties of which the CA is aware;

- conclude the issuance and distribution of certificates and CRLs;

- generate a new BYGCA certificate with a new key pair that will be soon available on the website.

If an RA Operator's private key is compromised or suspected to be compromised, the RA Operator or Manager must inform the BYGCA and request the revocation of the RA Operator's certificate.

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

No stipulation.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA Termination

Before the BYGCA terminates its services, it will:

– inform the Registration Authorities, subscribers and relying parties of which the BYGCA is aware;

– make information of its termination available on it's website;

– stop issuing certificates;

– annihilate all copies of private keys.

Before the BYGCA RA terminates its services, it will:

– inform the BYGCA;

– make information of its termination available on its and the BYGCA website;

– stop accepting certificate requests.

An advance notice of no less than 60 days will be given in the case of normal (scheduled) CA or RA termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keys for the BYGCA root certificate are generated on a dedicated machine, not connected to any type of network. The software used for key generation is EJBCA. Each subscriber must generate his/her own key pair.

6.1.2 Private key delivery to subscriber

As each applicant generates his/her own key pair, the BYGCA has no access to subscribers' private keys.

6.1.3 Public key delivery to certificate issuer

Defined in 4.1.2.

6.1.4 CA public key delivery to relying parties

The BYGCA root certificate is available on the website defined in section 2.1.

6.1.5 Key Sizes

For a user or host certificate the key size is 1024 or 2048 bits. The BYGCA key size is 2048 bits.

6.1.6 Public key parameters generation

No stipulation.

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

Keys may be used for authentication, data encipherment, message integrity and session establishment.

The BYGCA private key will only be used to issue CRLs and new certificates.

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

A backup of the BYGCA private key is kept encrypted in multiple copies in USB flash drive and CD-ROM. The password for the private key is kept separately in paper form with an access control. Only authorized personnel of the BYGCA have access to the backups.

6.2.5 Private key archival

The BYGCA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

The BYGCA does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

Same as in section 6.2.6.

6.2.8 Method of activating private key

The private key of the BYGCA is activated by using a passphrase. 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 BYGCA, all media that contain the private key of the BYGCA will be securely and permanently destroyed, according to then best current practice.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

No stipulation.

6.3.1 Public Key Archival

Public keys of all issued certificates are archived as a part of certificate archival.

6.3.2 Certificate operational periods and key pair usage periods

The BYGCA root certificate has a validity of twenty years. For subscribers, the maximum validity period for a certificate is one year plus one month.

6.4 Activation Data

6.4.1 Activation data generation and installation

The BYGCA does not generate activation data for subscribers. It's upon the subscriber to generate a strong passphrase, in order to be used as activation data for his/her private key.

The BYGCA private key is protected with a passphrase of at least 15 elements and that is known only by designated personnel of the BYGCA.

31

6.4.2 Activation data protection

The subscriber is responsible to protect the activation data for his/her private key. The BYGCA uses a passphrase to activate its private key which is known only by the BYGCA manager and the BYGCA operators. A copy in written form of the passphrase is sealed in an envelope and kept in a safe. Access to the safe is restricted only to the BYGCA manager and operators. Change of the BYGCA staff will imply change of passphrase. Old activation data are destroyed according to current best practices.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Computers operating at the BYGCA meet the following requirements:

– the signing mashine is kept off between uses;

– operating systems are maintained at a high level of security by applying in a timely manner all recommended and applicable security patches;

– monitoring is done to detect unauthorized software changes;

– system services are reduced to the bare minimum.

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

Certificates are issued on a machine not connected to any kind of network. Protection of other machines is provided by firewalls.

6.8 Time stamping

No stipulation.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3.

7.1.2 Certificate Extensions

The BYGCA supports and uses the following X.509 v3 Certificate extensions. For CA root certificate the extensions are:

– X509v3 Basic Constraints: critical, CA:TRUE

– X509v3 Key Usage: critical, CRL Sign, Key Cert Sign

– X509v3 Subject Key Identifier: <CA key ID>

– X509v3 Authority Key Identifier: keyid:<CA key ID>

For user certificate the extensions are:

– X509v3 Basic Constraints: critical, CA:FALSE

– X509v3 Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment

– X509v3 Extended Key Usage: TLS Web Client Authentication, E-mail Protection

– X509v3 Subject Key Identifier: <subject key ID>

– X509v3 Authority Key Identifier: keyid:<CA key ID>

– X509v3 Subject Alternative Name: email:<user's email address>

– X509v3 Certificates Policies: Policy: <OID of the effective CP/CPS>

– X509v3 CRL Distribution Points: URI:http://ca.grid.by/bygca-crl.crl

In case of host and service certificates the extensions are:

– X509v3 Basic Constraints: critical, CA:FALSE

– X509v3 Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment

– X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication

– X509v3 Subject Key Identifier: <subject key ID>

– X509v3 Authority Key Identifier: keyid:<CA key ID>

– X509v3 Subject Alternative Name: DNS:FQDN

– X509v3 Certificates Policies: Policy: <OID of the effective CP/CPS>

– X509v3 CRL Distribution Points: URI:http://ca.grid.by/bygca-crl.crl

7.1.3 Algorithm Object Identifiers

For the message digest that protects the certificate integrity, known-weak signatures or hash functions, such as MD5, must not be used. The current most secure hash function that is supported by the entire target audience of the BYGCA should be used, but at least SHA-1 or better must be used.

7.1.4 Name Forms

Issuer: DC=by, DC=grid, O=uiip.bas-net.by, CN= Belarusian Grid Certification Authority

Natural persons: DC=by, DC= grid, O=domain.by, CN=Firstname Lastname

Hosts: DC=by, DC= grid, O=domain.by, CN=fully.qualified.domain.name

Services: DC=by, DC=grid, O=domain.by, CN=servicename/fully.qualified.domain.name

The "CN" field structure for the user or host/service are described in section 3.1.

In case of person, the CN part of DN can contain only English alphabet letters, numbers and following special characters: left round bracket ('('), right round bracket (')'), space (' ') and hyphen ('-'). In case of host and service, the CN part of DN can contain only English alphabet letters, numbers and following special characters: dot ('.') and hyphen ('-'). Additionally, in case of grid host certificate and service certificate character '/' can be used. The maximal length of the CN is 64 characters for all types of certificates.

The DN is encoded as PrintableString as defined in RFC 2252.

7.1.5 Name constraints

See section 3.1.2.

7.1.6 Certificate Policy Object Identifier

See section 1.2.

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)

All CRLs will be issued in X.509 version 2.

7.2.2 CRL and CRL entry extensions

The BYGCA supports and uses the following CRL and CRL entry extensions:

– authorityKeyIdentifier: unique identifier of the issuer key according to RFC 3280;

– cRLNumber: monotonically increasing sequence number for each CRL issued by the CA according to RFC 3280.

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 BYGCA must allow to be audited by the EUGridPMA members 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. The BYGCA will perform operational audit of the CA/RA staff at least once per year.

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

In case of a deficiency, the BYGCA will announce the steps that will be taken to remedy the deficiency. This announcement will include a timetable. 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

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

Same as section in 9.1.1.

9.1.3 Revocation or status information access fees

Same as section in 9.1.1.

9.1.4 Fees for other services

Same as section in 9.1.1.

9.1.5 Refund policy

No fees shall be charged so there is no refund policy.

9.2 Financial responsibility

The BYGCA denies any financial responsibilities for damages or impairments resulting from its operation.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

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.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

The BYGCA collects information about the subscribers.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

The BYGCA collects a photocopy of an ID documents provided which is considered as private and will be kept confidential.

9.4.3 Information not deemed private

The BYGCA collects the following information which is not deemed as private:
- subscriber's e-mail address;
- subscriber's name;
- subscriber's organization;
- subscriber's certificate.

Statistics regarding certificates issuance and revocation don't contain any personal information and is not considered confidential.

9.4.4 Responsibility to protect private information

The BYGCA has the responsibility to protect the private information defined in section 9.4.2. The photocopies of ID documents will be kept private in a safe by the BYGCA and

will be only used while the audit process. The data from the photocopied documents will not be processed for any other purposes.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

1. RFC 3647;
2. UK e-Science CA CP/CPS;
3. Macedonian Academic and Research Grid Initiative CA CP/CPS;
4. Baltic Grid CA CP/CPS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The BYGCA is solely responsible for the issuance and management of certificates referencing this CP/CPS. The BYGCA shall:

– handle certificate requests and issue new certificates:

- confirm certification requests from entities requesting a certificate according to the procedures described in this CP/CPS;
- issue certificates based on requests from authenticated entities;
- send notification of issued certificates to requesting entities and corresponding RA;

– handle certificate revocation requests and certificate revocation:

- confirm revocation requests from entities requesting that a certificate be revoked according to the procedures described in this CP/CPS;
- issue CRLs;
- make certificate revocation information publicly available;
- publish BYGCA's root of trust to a trust anchor repository defined by EUGridPMA.

9.6.2 RA representations and warranties

Each RA shall:

- accept conditions and adhere to the procedures described in this CP/CPS;
- handle certificate requests:

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

  - authenticate the identity of the person requesting a certificate and reject the request if the certificate applicant does not pass the authentication;

  - check that the subscriber knows and agrees to subscriber obligations as defined in 9.6.3;

  - approve certificate requests;

  - notify the BYGCA that a certificate request is authenticated and approved;

- handle certificate revocation requests:

  - verify that the information provided in the certificate revocation request is correct;

  - approve revocation requests;

  - notify the BYGCA that the certificate revocation request is authenticated and approved.

9.6.3 Subscriber representations and warranties

In requesting a certificate, subscribers agree to:

- accept conditions and adhere to the procedures described in this CP/CPS;

- provide true and accurate information to the BYGCA and only such information as he/she is entitled to submit for the purposes of this CP/CPS;

- use the certificate exclusively for authorized and legal purposes, consistent with this CP/CPS;

- by using the authentication procedures described in this CP/CPS subscribers accept the restrictions to liability;

- by using the authentication procedures described in this CP/CPS subscribers accept the statements relating to confidentiality of information in section 9.3;

- generate a key pair using a trustworthy method;

- use strong passphrase to protect private key of user certificate;

- ensure that private key of host or service certificate is readable only by root or a restricted user account;

- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate;

- notify the BYGCA immediately in case a private key is lost or compromised.

9.6.4 Relying party representations and warranties

In using a certificate issued by the BYGCA relying parties agree to:

- accept conditions and adhere to the procedures described in this CP/CPS

- verify the certificate revocation information before using a certificate

– use the certificate exclusively for authorized and legal purposes, consistent with this CP/CPS.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

1. The BYGCA guarantees to control the identity of the certification requests according to the procedures described in this document.

2. The BYGCA guarantees to control the identity of the revocation requests according to the procedures described in this document.

3. The BYGCA is run on a best effort basis and does not give any guarantees about the service security or suitability.

4. The BYGCA shall not be held liable for any problems arising from its operation or improper use of the issued certificates.

5. The BYGCA 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

9.12.1 Procedure for amendment

Subscribers will not be informed in advance if the CP/CPS document is changed. Changes are announced to the EUGridPMA and get approved before the new CP/CPS is declared on the website as defined in section 2.1. Changes are published on the website as well.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

OID must change whenever the version of CP/CPS document is updated.

9.13 Dispute resolution provisions

Legal disputes arising from the operation of the BYGCA will be resolved according to the laws of the Republic of Belarus.

9.14 Governing law

The enforceability, construction, interpretation, and validity of this policy shall be governed by the laws of the Republic of Belarus.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.