BG.ACAD | CA

Bulgarian Academic Certification Authority

Certificate Policy and Certification Practice Statement

Revision 1.0
OID: 1.3.6.1.4.1.26646.1.3.1.1.0

March 2007

1 INTRODUCTION 8
1.1 Overview 8
1.2 Document name and identification 8
1.3 PKI participants 8
1.3.1 Certification Authorities 8
1.3.2 Registration Authorities 9
1.3.3 Subscribers 9
1.3.4 Relying parties 9
1.3.5 Other participants 9
1.4 Certificate usage 10
1.4.1 Appropriate certificate usage 10
1.4.2 Inappropriate certificate usage 10
1.5 Policy administration 10
1.5.1 Organization administering the document 10
1.5.2 Contact Person 10
1.5.3 Person determining CPS suitability for the policy 11
1.5.4 CPS approval procedures 11
1.6 Definitions and acronyms 11
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 13
2.1 Repositories 13
2.2 Publication of certification information 13
2.3 Time or frequency of publication 13
2.4 Access control on repositories 14
3 IDENTIFICATION AND AUTHENTICATION 15
3.1 Naming 15
3.1.1 Types of names 15
3.1.2 Need for names to be meaningful 16
3.1.3 Anonymity or pseudonymity of subscribers 16
3.1.4 Rules for interpreting various name forms 16
3.1.5 Uniqueness of names 16
3.1.6 Recognition, authentication, and role of trademarks 16
3.2 Initial identity validation 16
3.2.1 Method to prove possession of key 16
3.2.2 Authentication of organization identity 16
3.2.3 Authentication of individual identity 17
3.2.4 Non-verified subscriber information 17
3.2.5 Validation of Authority 17
3.2.6 Criteria of interoperation 17
3.3 Identification and authentication for re-key requests 17
3.3.1 Identification and authentication for routine re-key 17
3.3.2 Identification and authentication for re-key after revocation 17
3.4 Identification and authentication for revocation request 17
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 19
4.1 Certificate application 19
4.1.1 Who can submit a certificate application 19
4.1.2 Enrollment process and responsibilities 19
4.2 Certificate application processing 20
4.2.1 Performing identification and authentication functions 20
4.2.2 Approval or rejection of certificate applications 20

4.2.3 Time to process certificate applications 20
4.3 Certificate issuance 20
4.3.1 CA actions during certificate issuance 20
4.3.2 Notification to subscriber by the CA of issuance of certificate 20
4.4 Certificate acceptance 21
4.4.1 Conduct constituting certificate acceptance 21
4.4.2 Publication of the certificate by the CA 21
4.4.3 Notification of certificate issuance by the CA to other entities 21
4.5 Key pair and certificate usage 21
4.5.1 Subscriber private key and certificate usage 21
4.5.2 Relying party public key and certificate usage 21
4.6 Certificate renewal 21
4.6.1 Circumstance for certificate renewal 21
4.6.2 Who may request renewal 21
4.6.3 Processing certificate renewal requests 21
4.6.4 Notification of new certificate issuance to subscriber 21
4.6.5 Conduct constituting acceptance of a renewal certificate 22
4.6.6 Publication of the renewal certificate by the CA 22
4.6.7 Notification of certificate issuance by the CA to other entities 22
4.7 Certificate re-key 22
4.7.1 Circumstance for certificate re-key 22
4.7.2 Who may request certification of a new public key 22
4.7.3 Processing certificate re-keying requests 22
4.7.4 Notification of new certificate issuance to subscriber 22
4.7.5 Conduct constituting acceptance of a re-keyed certificate 22
4.7.6 Publication of the re-keyed certificate by the CA 22
4.7.7 Notification of certificate issuance by the CA to other entities 23
4.8 Certificate modification 23
4.8.1 Circumstance for certificate modification 23
4.8.2 Who may request certificate modification 23
4.8.3 Processing certificate modification requests 23
4.8.4 Notification of new certificate issuance to subscriber 23
4.8.5 Conduct constituting acceptance of modified certificate 23
4.8.6 Publication of the modified certificate by the CA 23
4.8.7 Notification of certificate issuance by the CA to other entities 23
4.9 Certificate revocation and suspension 23
4.9.1 Circumstances for revocation 23
4.9.2 Who can request revocation 23
4.9.3 Procedure for revocation request 23
4.9.4 Revocation request grace period 24
4.9.5 Time within which CA must process the revocation request 24
4.9.6 Revocation checking requirement for relying parties 24
4.9.7 CRL issuance frequency 24
4.9.8 Maximum latency for CRLs 24
4.9.9 On-line revocation/status checking availability 24
4.9.10 On-line revocation checking requirements 24
4.9.11 Other forms of revocation advertisements available 24
4.9.12 Special requirements re key compromise 24
4.9.13 Circumstances for suspension 24
4.9.14 Who can request suspension 24

4.9.15 Procedure for suspension request 24
4.9.16 Limits on suspension period 24
4.10 Certificate status services 24
4.10.1 Operational characteristics 24
4.10.2 Service availability 25
4.10.3 Optional features 25
4.11 End of subscription 25
4.12 Key escrow and recovery 25
4.12.1 Key escrow and recovery policy and practices 25
4.12.2 Session key encapsulation and recovery policy and practices 25
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 26
5.1 Physical controls 26
5.1.1 Site location and construction 26
5.1.2 Physical access 26
5.1.3 Power and air conditioning 26
5.1.4 Water exposures 26
5.1.5 Fire prevention and protection 26
5.1.6 Media storage 26
5.1.7 Waste disposal 26
5.1.8 Off-site backup 26
5.2 Procedural controls 26
5.2.1 Trusted roles 26
5.2.2 Number of persons required per task 27
5.2.3 Identification and authentication for each role 27
5.2.4 Roles requiring separation of duties 27
5.3 Personnel controls 27
5.3.1 Qualifications, experience, and clearance requirements 27
5.3.2 Background check procedures 27
5.3.3 Training requirements 27
5.3.4 Retraining frequency and requirements 27
5.3.5 Job rotation frequency and sequence 27
5.3.6 Sanctions for unauthorized actions 27
5.3.7 Independent contractor requirements 27
5.3.8 Documentation supplied to personnel 27
5.4 Audit logging procedures 28
5.4.1 Types of events recorded 28
5.4.2 Frequency of processing log 28
5.4.3 Retention period for audit log 28
5.4.4 Protection of audit log 28
5.4.5 Audit log backup procedures 28
5.4.6 Audit collection system (internal vs. external) 28
5.4.7 Notification to event-causing subject 28
5.4.8 Vulnerability assessments 28
5.5 Records archival 28
5.5.1 Types of records archived 28
5.5.2 Retention period for archive 29
5.5.3 Protection of archive 29
5.5.4 Archive backup procedures 29
5.5.5 Requirements for time-stamping of records 29
5.5.6 Archive collection system (internal or external) 29

5.5.7 Procedures to obtain and verify archive information 29
5.6 Key changeover 29
5.7 Compromise and disaster recovery 29
5.7.1 Incident and compromise handling procedures 29
5.7.2 Computing resources, software, and/or data are corrupted 30
5.7.3 Entity private key compromise procedures 30
5.7.4 Business continuity capabilities after a disaster 30
5.8 CA or RA termination 30
6 TECHNICAL SECURITY CONTROLS 31
6.1 Key pair generation and installation 31
6.1.1 Key pair generation 31
6.1.2 Private key delivery to subscriber 31
6.1.3 Public key delivery to certificate issuer 31
6.1.4 CA public key delivery to relying parties 31
6.1.5 Key sizes 31
6.1.6 Public key parameters generation and quality checking 31
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 31
6.2 Private Key Protection and Cryptographic Module Engineering Controls 32
6.2.1 Cryptographic module standards and controls 32
6.2.2 Private key (n out of m) multi-person control 32
6.2.3 Private key escrow 32
6.2.4 Private key backup 32
6.2.5 Private key archival 32
6.2.6 Private key transfer into or from a cryptographic module 32
6.2.7 Private key storage on cryptographic module 32
6.2.8 Method of activating private key 32
6.2.9 Method of deactivating private key 32
6.2.10 Method of destroying private key 32
6.2.11 Cryptographic Module Rating 32
6.3 Other aspects of key pair management 32
6.3.1 Public key archival 32
6.3.2 Certificate operational periods and key pair usage periods 33
6.4 Activation data 33
6.4.1 Activation data generation and installation 33
6.4.2 Activation data protection 33
6.4.3 Other aspects of activation data 33
6.5 Computer security controls 33
6.5.1 Specific computer security technical requirements 33
6.5.2 Computer security rating 34
6.6 Life cycle technical controls 34
6.6.1 System development controls 34
6.6.2 Security management controls 34
6.6.3 Life cycle security controls 34
6.7 Network security controls 34
6.8 Time-stamping 34
7 CERTIFICATE, CRL, AND OCSP PROFILES 35
7.1 Certificate profile 35
7.1.1 Version number(s) 35
7.1.2 Certificate extensions 35
7.1.3 Algorithm object identifiers 35

7.1.4 Name forms 35
7.1.5 Name constraints 35
7.1.6 Certificate policy object identifier 35
7.1.7 Usage of Policy Constraints extension 35
7.1.8 Policy qualifiers syntax and semantics 35
7.1.9 Processing semantics for the critical Certificate Policies extension 36
7.2 CRL profile 36
7.2.1 Version number(s) 36
7.2.2 CRL and CRL entry extensions 36
7.3 OCSP profile 36
7.3.1 Version number(s) 36
7.3.2 OCSP extensions 36
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 37
8.1 Frequency or circumstances of assessment 37
8.2 Identity/qualifications of assessor 37
8.3 Assessor's relationship to assessed entity 37
8.4 Topics covered by assessment 37
8.5 Actions taken as a result of deficiency 37
8.6 Communication of results 37
9 OTHER BUSINESS AND LEGAL MATTERS 38
9.1 Fees 38
9.1.1 Certificate issuance or renewal fees 38
9.1.2 Certificate access fees 38
9.1.3 Revocation or status information access fees 38
9.1.4 Fees for other services 38
9.1.5 Refund policy 38
9.2 Financial responsibility 38
9.2.1 Insurance coverage 38
9.2.2 Other assets 38
9.2.3 Insurance or warranty coverage for end-entities 38
9.3 Confidentiality of business information 38
9.3.1 Scope of confidential information 38
9.3.2 Information not within the scope of confidential information 38
9.3.3 Responsibility to protect confidential information 38
9.4 Privacy of personal information 38
9.4.1 Privacy plan 39
9.4.2 Information treated as private 39
9.4.3 Information not deemed private 39
9.4.4 Responsibility to protect private information 39
9.4.5 Notice and consent to use private information 39
9.4.6 Disclosure pursuant to judicial or administrative process 39
9.4.7 Other information disclosure circumstances 39
9.5 Intellectual property rights 39
9.6 Representations and warranties 39
9.6.1 CA representations and warranties 39
9.6.2 RA representations and warranties 39
9.6.3 Subscriber representations and warranties 39
9.6.4 Relying party representations and warranties 40
9.6.5 Representations and warranties of other participants 40
9.7 Disclaimers of warranties 40

9.8 Limitations of liability 40
9.9 Indemnities 40
9.10 Term and termination 40
9.10.1 Term 40
9.10.2 Termination 40
9.10.3 Effect of termination and survival 40
9.11 Individual notices and communications with participants 40
9.12 Amendments 40
9.12.1 Procedure for amendment 40
9.12.2 Notification mechanism and period 40
9.12.3 Circumstances under which OID must be changed 40
9.13 Dispute resolution provisions 41
9.14 Governing law 41
9.15 Compliance with applicable law 41
9.16 Miscellaneous provisions 41
9.16.1 Entire agreement 41
9.16.2 Assignment 41
9.16.3 Severability 41
9.16.4 Enforcement (attorneys' fees and waiver of rights) 41
9.16.5 Force Majeure 41
9.17 Other provisions 41

1 INTRODUCTION

1.1 Overview

The *Bulgarian Academic Certification Authority* (BG.ACAD CA*)* is established to serve the needs of the research and education community in Bulgaria for PKI services. These needs might emerge either from the general operations of the academic entities (e.g. deployment of various network services, eLearning programmes, eContent hosting, etc.) or from specific projects and activities (e.g. deployment of computational and data GRIDs, the *eduroam* framework, etc.) *BG.ACAD CA* is thus supposed to be the single Certification Authority on the academic field in the Republic of Bulgaria, providing stable services with long-term commitment to the largest possible user community.

BG.ACAD CA is hosted at the *Institute for Parallel Processing at the Bulgarian Academy of Sciences* (IPP-BAS), and operated by the *Distributed Systems and Networking Department* as part of the services oriented towards the academic community (NOC, CSIRT, etc.). *BG.ACAD 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 *BG.ACAD 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

- Title
  “*BG.ACAD CA Certificate Policy and Certification Practice Statement*”
- Revision
  1.0
- Date issued
  05 March 2007
- OID

```
1.3.6.1.4.1.26646.1.3.1.1.0
----------- ----- - - - - -
     |        |   | | | | +- minor version
     |        |   | | | +--- major version
     |        |   | | +----- CP/CPS document
     |        |   | +------- CA
     |        |   +--------- BG.ACAD
     |        +------------- IPP-BAS
     +---------------------- IANA
```

1.3 PKI participants

1.3.1 Certification Authorities

BG.ACAD CA is defined as a medium security CA. The only entities authorized to issue certificates on its behalf are persons who are formally assigned staff members responsible for the operation of *BG.ACAD CA*. Their list is published in the secure online repository (as described in section **2.2**), and is updated regularly. There shall be no subordinate certification authorities. Distribution of the validation process shall be implemented using a network of trusted Registration Authorities (RAs).

1.3.2 Registration Authorities

Certain individuals can be recognized by *BG.ACAD CA* to act as trusted intermediaries in the identity verification process between the subscriber and the Certification Authority. Such trusted intermediaries are formally assigned by *BG.ACAD 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.

1.3.3 Subscribers

Certificates may be issued both to individuals and to computer entities. Eligible for certification by *BG.ACAD CA* are:

- Individuals working for organizations formally based in and/or having offices inside the Republic of Bulgaria that exclusively operate in the research and/or education field (e.g. universities, schools, research institutes of the Bulgarian Academy of Sciences, their subordinates and divisions, etc.). Employees of other organizations, not directly involved in the research and/or education field, qualify under this Policy if the said organization operates for non-commercial purposes on a not-for-profit basis.
- Computer entities (that is, digital information processing devices, capable of performing cryptographic operations) used in the operational activities of the aforementioned organizations. Computer entities that are not directly related to the organization’s operations are not eligible for certification.
- Individuals or computer entities, 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 said computer entities; however, a host certificate shall be preferred to a service one in all cases where the latter is not strictly required.

The services, provided by *BG.ACAD CA*, are non-discriminatory and shall be provided to all qualified entities under the same conditions and at the same service level.

1.3.4 Relying parties

All entities (including users of the Grid computing infrastructures) that employ the public keys in certificates, issued by *BG.ACAD 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 *BG.ACAD 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 *BG.ACAD CA* for financial transactions or in violation of the state or international law is strictly forbidden.

1.5 Policy administration

1.5.1 Organization administering the document

The *BG.ACAD CA* CP/CPS is authored and administered by the Distributed Systems and Networking Department at IPP-BAS.

The address of *BG.ACAD CA* for operational issues is:

BULGARIAN ACADEMIC
CERTIFICATION AUTHORITY
Distributed Systems and Networking Dept.
Institute for Parallel Processing
Bulgarian Academy of Sciences
25A Acad G Bontchev Str
1113 Sofia
BULGARIA

Phone:	+359 2 9796614
Fax:	+359 2 8707273
Email:	operations@ca.acad.bg

1.5.2 Contact Person

The contact person for questions about this CP/CPS document or any other *BG.ACAD CA* related issues is:

Luchesar V. ILIEV
Distributed Systems and Networking Dept.
Institute for Parallel Processing
Bulgarian Academy of Sciences
25A Acad G Bontchev Str
1113 Sofia
BULGARIA

Phone:	+359 2 9796614
Fax:	+359 2 8707273
Email:	iliev@acad.bg

1.5.3 Person determining CPS suitability for the policy

The person determining the CPS suitability for the policy is:

Luchesar V. ILIEV
Distributed Systems and Networking Dept.
Institute for Parallel Processing
Bulgarian Academy of Sciences
25A Acad G Bontchev Str
1113 Sofia
BULGARIA

Phone: +359 2 9796614
Fax: +359 2 8707273
Email: iliev@acad.bg

1.5.4 CPS approval procedures

No stipulation.

1.6 Definitions and acronyms

The following definitions and acronyms are used in this document:

Certificate
Synonymous with Public Key Certificate.

Certification Authority (CA)
An entity trusted by one or more users to create and assign public key certificates and be responsible for them during their whole lifetime.

Certificate Policy (CP)
A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certification Practice Statement (CPS)
A statement of the practices which a certification authority employs in issuing certificates.

Certificate Revocation List (CRL)
A time-stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

Public Key Certificate
A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA that issued it.

Registration Authority (RA)
An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or

issue certificates (i.e. an RA is delegated certain tasks on behalf of the CA).

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms “certificate user” and “relying party” are used interchangeably.

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 *BG.ACAD CA* are operated by the Distributed Systems and Networking Department at IPP-BAS.

The address of *BG.ACAD CA* for issues regarding the repositories is:

BULGARIAN ACADEMIC
CERTIFICATION AUTHORITY
Distributed Systems and Networking Dept.
Institute for Parallel Processing
Bulgarian Academy of Sciences
25A Acad G Bontchev Str
1113 Sofia
BULGARIA

Phone:	+359 2 9796614
Fax:	+359 2 8707273
Email:	repositories@ca.acad.bg

2.2 Publication of certification information

BG.ACAD 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.acad.bg/

It contains:

- the *BG.ACAD 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 document, under which certificates have been issued;
- the current list of the formally assigned staff members of *BG.ACAD 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 *BG.ACAD CA* itself;
- other information relating 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 issued by *BG.ACAD CA* that reference this Policy and CRLs shall be published as soon as possible after their issuance. All other information shall be published promptly after its update or after it becomes available to the CA.

2.4 Access control on repositories

BG.ACAD CA does not impose any access control restrictions on the information available at its online repository. However, *BG.ACAD CA* reserves the right 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 DN under this CP/CPS shall start with "DC=bg, DC=acad". 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 *BG.ACAD 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. When the name in Latin does not adhere to the PrintableString definition of RFC 2252, excluding comma, double quote, and single quote characters, an appropriate transliteration shall be performed (e.g. ligatures converted to separate letters, diacritics dropped, etc.) Transliteration shall also be performed when the name is not available in Latin letters from the ID document.

  There must be at least two distinct (separated by spaces) parts in the name. Where the full name consists of three or more such parts, the middle one(s) (e.g. *father's name* as per Republic of Bulgaria's official Identity Card) may be abbreviated to its/their first letter; period shall be written after such abbreviations (e.g. *Aleko I. Konstantinov, John R. R. Tolkien*). Non-distinct parts separated by hyphens (e.g. *Anna-Maria, Whalley-Kilmer*) must be written in their completeness.

  When the subscriber has a strong reason 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. 007) 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 DN. 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 adhere to 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 adhere to 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 subject name must represent the subscriber in a way that is easily understandable by humans, and must have a reasonable association with the authenticated name of the subscriber.

3.1.3 Anonymity or pseudonymity of subscribers

BG.ACAD 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

BG.ACAD CA shall guarantee that each subject name is globally unique and never assigned to more than one entity. 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

BG.ACAD CA proves possession of the private key of its own root certificate by issuing certificates and signing CRLs.

BG.ACAD 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.

BG.ACAD 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

BG.ACAD CA (or an RA on its behalf) shall authenticate organizations based on suitable official documents, e.g. a signed and stamped copy of the organization's registration required by the Bulgarian law. Additional documents may be required or checks may be made to ensure that the organization conforms to the requirements of section **1.3.3**.

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.

In case the entity is a natural person, the initial authentication shall be based on government-issued identification documents (ID card, driving license, or passport) and physical appearance of the applicant before the CA or RA.

In case the entity to be certified is a machine or software component, the requester (a natural person) must prove to the satisfaction of the CA (or the RA on CA’s behalf) 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.

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

Re-key before expiration can be accomplished by sending a re-key e-mail request, signed with the current user certificate. Re-key after expiration follows the same authentication procedure as for a new certificate.

3.3.2 Identification and authentication for re-key after revocation

A revoked key shall not be re-certified. The authentication of a new certificate request follows the rules specified in section **3.2.3**.

3.4 Identification and authentication for revocation request

A revocation request needs to be authenticated, unless *BG.ACAD CA* can independently verify that the case is one of the listed in section **4.9.1**. Certificate revocation requests should be submitted via e-mail.

In case the revocation request is for a user certificate, the e-mail must be signed by the private key, corresponding to the certificate that is requested to be revoked, which must be a valid, non-expired, non-revoked certificate, issued by

BG.ACAD CA. If the revocation request is for a host or service certificate, then the e-mail must be signed by the private key corresponding to a valid, non-expired, non-revoked *BG.ACAD CA* certificate of the person responsible for the given host or service, as ascertained during the authentication process (section **3.2.3**).

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 2048 bits and the validity of the requested certificate must be at most one year plus one month. *BG.ACAD CA* will never generate a key pair for an applicant, nor will it accept secret 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 18 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

For the first time and after that once every 3 years, a subscriber must be authenticated by the RA serving his/her location 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 *BG.ACAD CA*; *c*) shall protect the relevant private key(s) in accordance with the rules of this Policy, and *d*) assumes the responsibility to notify *BG.ACAD 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 *BG.ACAD CA* via a signed and encrypted e-mail, accompanied with a phone call to the relevant *BG.ACAD 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 *BG.ACAD CA*. Else, 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 *BG.ACAD 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 from the *BG.ACAD 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 *BG.ACAD CA* certificate (subject to the 3-year period described in section **4.1.2**).

4.2.2 Approval or rejection of certificate applications

The necessary provisions, which must be followed for any certificate application request to *BG.ACAD CA* in order to be approved, are:

- the certificate application must first be successfully authenticated;
- the subscriber must apply the certificate request with the correct random code within 5 working days after a successful initial authentication performed by the RA, unless he/she has already applied it during authentication;
- the subject must be an acceptable entity as defined by this Policy;
- the request must obey to the *BG.ACAD CA* distinguished name scheme;
- the distinguished name must be unambiguous and unique;
- the certificate key must have at least 2048 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 *BG.ACAD 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 *BG.ACAD 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 *BG.ACAD 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 certificates, issued by *BG.ACAD 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 those described in section **1.4.2**.

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 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

BG.ACAD 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

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

4.6.3 Processing certificate renewal requests

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

4.6.4 Notification of new certificate issuance to subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

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

4.6.6 Publication of the renewal certificate by the CA

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

4.6.7 Notification of certificate issuance by the CA to other entities

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

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Subscribers should regenerate their key pair in the following circumstances:

- expiration of their certificate signed by *BG.ACAD CA*;
- revocation of their certificate by *BG.ACAD 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

Re-key before expiration shall be accomplished by sending a re-key request signed with the current user certificate. 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 *BG.ACAD CA* online repository at this time, shall be assumed.

BG.ACAD 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.

In any case, at least once every 3 years the subscriber must go through the procedure as for a new certificate.

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 *BG.ACAD 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

No stipulation.

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 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:

- 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 entity requesting the certificate revocation shall be authenticated by signing the revocation request with a valid *BG.ACAD CA* certificate. If such certificate is not available or cannot be used, 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

BG.ACAD CA shall process all revocation requests in the timeliest manner. Under no circumstances a revocation request shall take more than one working day to process.

4.9.6 Revocation checking requirement for relying parties

Relying parts must 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

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

4.9.8 Maximum latency for CRLs

The CRL shall be issued immediately 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

BG.ACAD CA does not suspend certificates.

4.9.14 Who can request suspension

BG.ACAD CA does not suspend certificates.

4.9.15 Procedure for suspension request

BG.ACAD CA does not suspend certificates.

4.9.16 Limits on suspension period

BG.ACAD CA does not suspend certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

BG.ACAD CA operates an online repository that 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

BG.ACAD CA will not accept secret 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

BG.ACAD CA operates in a restricted access, monitored areas, located in the *Institute for Parallel Processing of the Bulgarian Academy of Sciences* (IPP-BAS). *BG.ACAD CA* signing machine and the repository web server are entirely dedicated to these roles. The signing machine furthermore is not connected to any form of computer network.

5.1.2 Physical access

Physical access to *BG.ACAD CA* sites is restricted to the authorized personnel only, and the areas are under constant monitoring. The signing system is furthermore kept in a locked strongbox when not in use.

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 *BG.ACAD CA* facilities, floods are not expected.

5.1.5 Fire prevention and protection

All facilities of the IPP-BAS adhere to the Bulgarian law regarding fire prevention and protection in public buildings. The signing machine is furthermore located in a room with automatic, industrial-grade fire detection and suppression system.

5.1.6 Media storage

Backup copies of *BG.ACAD 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, carrying 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 *BG.ACAD 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

There must be at least 3 persons capable of signing operations.

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

BG.ACAD CA personnel must consist of suitably trained persons who are familiar with the PKI infrastructure and operation, and who possess the relevant technical and professional competence. At least one of them must be a BG.ACAD CERT team member. 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 *BG.ACAD CA* personnel.

5.3.4 Retraining frequency and requirements

BG.ACAD 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 escalation (“su root”)
- other important system information (e.g. kernel messages, etc.)

In general:

- requests for certificate
- 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 *BG.ACAD CA* personnel is allowed to access and process audit logs. The audit logs never leave *BG.ACAD 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 *BG.ACAD 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 *BG.ACAD 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 *BG.ACAD CA* personnel is allowed access to the record archives. The archives never leave *BG.ACAD 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 *BG.ACAD 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 *BG.ACAD CA*.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

BG.ACAD 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 root certificate shall be available to verify old signatures, and the old secret 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 *BG.ACAD CA* private key is compromised or suspected to be compromised, or if it is destroyed, *BG.ACAD CA* shall immediately:

- notify the subscribers and the RAs, as well as the relevant relying parties of which/whom *BG.ACAD 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 the BG.ACAD CERT team;

- notify all other relevant security contacts.

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

The private keys of *BG.ACAD 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 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, *BG.ACAD CA* shall:

- notify the subscribers and the RAs, as well as the relevant relying parties of which/whom *BG.ACAD 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 *BG.ACAD CA* are generated exclusively by authorized *BG.ACAD 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.

BG.ACAD CA does not generate private keys on behalf of subscribers. The subscribers' private keys must never be sent to *BG.ACAD 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 *BG.ACAD 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 *BG.ACAD 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 2048 bits. The minimum length for *BG.ACAD 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)

BG.ACAD 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 *BG.ACAD 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

BG.ACAD 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

BG.ACAD CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

BG.ACAD CA does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

BG.ACAD CA does not use any kind of cryptographic module.

6.2.8 Method of activating private key

The private key of *BG.ACAD 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 or after the archival period for archives has expired, 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 *BG.ACAD CA* shall have a maximum lifetime of one year plus one month. The lifetime of *BG.ACAD CA* root certificate shall be no more than 20 years and no less than 3 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The pass phrase used to activate the *BG.ACAD CA* private key is generated on the computer used for the CA signing operations. It must be at least 30 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.

BG.ACAD CA does not generate activation data for subscribers. It is upon the subscriber to generate a secure pass phrase, at least 18 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 *BG.ACAD CA* signing key is known only to the authorized *BG.ACAD 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.
- The *BG.ACAD CA* personnel are working in close coordination with the BG.ACAD CERT team to further minimize any possible security threats.

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 *BG.ACAD 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.
- Passive monitoring is performed in coordination with the BG.ACAD CERT team in order to detect malicious network activity.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All certificates that reference 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 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/serverAuth
  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.

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

The distinguished name of the CA is "DC=bg, DC=acad, CN=BG.ACAD CA". See section **3.1.1** for the name forms of subscriber certificates.

7.1.5 Name constraints

See section **3.1.1**.

7.1.6 Certificate policy object identifier

BG.ACAD CA identifies this Policy with the object identifier specified in 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 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

BG.ACAD 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. *BG.ACAD CA* may also be assessed for appropriate security measures by BG.ACAD CERT.

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

BG.ACAD 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

BG.ACAD 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

BG.ACAD CA does not collect any confidential or private information.

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

BG.ACAD 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
- SEE-GRID CA Certificate Policy and Certificate Practice Statement
- DutchGrid and NIKHEF Medium-security X.509 Certification Authority Certificate Policy and Certificate Practice Statement
- OGF’s Grid Certificate Profile (draft) revision 0.20
- AEGIS Certificate Policy and Certificate Practice Statement
- CERN Certification Authority Certificate Policy and Certification Practice Statement
- GridKa-CA Certificate Policy and Certification Practice Statement
- SWITCH Certificate Policy and Certification Practice 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

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

9.13 Dispute resolution provisions

Legal disputes arising from the operation of *BG.ACAD CA* shall be resolved according to the Bulgarian Law.

9.14 Governing law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the Laws of the Republic of Bulgaria.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

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.