AEGIS CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Table of Contents:

1. INTRODUCTION

This document describes the rules and procedures used by the AEGIS Certification Authority.

1.1 Overview

AEGIS (Academic and Educational Grid Initiative of Serbia) has been established on April 14, 2005. The main focus of AEGIS is:

- coordinate efforts to further develop academic and high performance computing facilities and help them integrate into AEGIS;
- organize dissemination and training activities and help Serbian research communities to develop and deploy applications that use AEGIS infrastructure;
- coordinate fund raising efforts to improve AEGIS infrastructure and human resources;
- facilitate wider participation of AEGIS members in Framework 6, Framework 7, and other international GRID projects;
- create a national GRID development policy;

Any additional information can be obtained at: http://aegis.phy.bg.ac.rs/
In order to stregthen AEGIS infrastructure and facilitate its efficient usage by Serbian research community, as well as to allow full integration of our user community and computing resources into the pan-European and other Grid infrastructures, it was necessary to establish AEGIS Certification Authority. The AEGIS CA will provide security infrastructure needed for the operation of all AEGIS resources and authentication of all AEGIS users, hosts and services.
This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the AEGIS Certification Authority (CA) in issuing certificates as well as the responsibilities of the involved parties.
The AEGIS CA is operated at the premises of University of Belgrade Computer Center.
This document is structured according to RFC 3647.
This document was issued on 04.03.2007, and took effect on 01.06.2007..

1.2 Document name and identification

Document title: AEGIS CA Certificate Policy and Certification Practice Statement
Document version: Version 1.3
Document date: 16.06.2011.
ASN.1 Object Identifier (OID): 1.3.6.1.4.1.11067.10.1.1.3
The next table describes the meaning of the OID:

1.3.6.1.4.1	Prefix for IANA private enterprises
11067	University of Belgrade registered identifier
10	Certification Authorities
1	CP/CPS
1.3	Major and minor CP/CPS number.

1.3 PKI participants

1.3.1 Certification Authorities

AEGIS certificates are signed by AEGIS CA. AEGIS CA provides PKI services to the Serbian academic and research communities who participate in national or international Grid activities. The AEGIS CA does not issue nor sign certificates to subordinate CAs.

1.3.2 Registration authorities

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 AEGIS CA website. Each RA will have it's own web interface.

1.3.3 Subscribers

The AEGIS CA issues user (personal), host and service certificates. Subscribers eligible for certification from AEGIS CA are:

- Users and site administrators of Academic and Educational Grid Initiative of Serbia (AEGIS).
- Computers used in activities of Academic and Educational Grid Initiative of Serbia (AEGIS).
- Services or host applications which are running on computers used in Academic and Educational Grid Initiative of Serbia (AEGIS).

1.3.4. Relying parties

Users of Grid computing infrastructures that are using the public keys, in certificates signed by the AEGIS 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 uses

Personal 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 certificates for email signing.

1.4.2 Prohibited certificate uses

Notwithstanding the above, using certificates for purposes contrary to Serbian law is explicitly prohibited.

1.5 Policy administration

1.5.1 Organization administering the document.

The AEGIS CA CP/CPS document was authored and is administered by the University of Belgrade Computer Center.
The AEGIS CA address for operations issues is:
AEGIS Certification authority
University of Belgrade Computer Center
Kumanovska 7
Belgrade 126119
Serbia
Phone: +381 11 3031257
Phone: +381 11 3031258
Fax: +381 11 3031259
e-mail: aegis-ca@aegis-ca.rcub.bg.ac.rs

1.5.2 Contact person

Contact person for questions related to this document or any other AEGIS CA related issue is:
Dušan Radovanović
University of Belgrade Computer Center
Kumanovska 7
Belgrade 126119
Serbia
Phone: +381 11 3031257
Phone: +381 11 3031258
Fax: +381 11 3031259
e-mail: dusan.radovanovic@rcub.bg.ac.rs

1.5.3 Person determining CPS suitability for the policy

Dušan Radovanović
University of Belgrade Computer Center
Kumanovska 7
Belgrade 126119
Serbia
Phone: +381 11 3031257
Phone: +381 11 3031258
Fax: +381 11 3031259
e-mail: dusan.radovanovic@rcub.bg.ac.rs

1.5.4 CPS approval procedures

The approved document shall be submitted to EUGridPMA for acceptance.

1.6 Definitions and acronyms

AEGIS	Academic and Educational Grid Initiative of Serbia

ASN.1	Abstract Syntax Notation One (http://asn1.elibel.tm.fr/)
CA	Certification Authority
CP/CPS	Certificate Policy/Certification Practice Statement
CRL	Certificate Revocation List
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
S/MIME	Secure / Multipurpose Internet Mail Extensions
SEE-GRID	South East European GRid-enabled eInfrastructure Development
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
USB	Universal Serial Bus

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The AEGIS CA operates an on-line repository that contains:

- The AEGIS CA root certificate
- User, Host and Service certificates issued by the CA.
- Certificate Revocation Lists (periodically updated)
- A copy of the most recent version of this CP/CPS
- A list of current operational Registration Authorities.
- Links to all trust anchor repositories where AEGIS CA info is published.
- Other relevant information http://aegis-ca.rcub.bg.ac.rs/

The AEGIS CA communication information for information regarding repositories is:
AEGIS Certification authority
University of Belgrade Computer Center
Kumanovska 7
Belgrade 126119
Serbia
Phone: +381 11 3031257
Phone: +381 11 3031258
Fax: +381 11 3031259
e-mail: aegis-ca@aegis-ca.rcub.bg.ac.rs

2.2 Publication of certification information

See section 2.1

2.3 Time or frequency of publication

- Certificates will be published as soon as they are issued.
- The published CRL will have a maximum lifetime of 30 days and it will be updated no later than 7 days before it's expiration date. In case of certificate revocation, the CRL will be updated immediately following the revocation.
- 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.
AEGIS CA may impose a more restricted access control policy to the repository at its discretion.
The AEGIS CA 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

The subject names for the certificate applicants shall follow the X.500 standard:

1. in case of user certificate the subject name must include the persons name in the CN field;
2. in case of host certificate the subject name must include the DNS FQDN in the CN field;
3. in case service certificate the subject name must include the service name and the DNS FQDN separated by a „/“ in the CN field.

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 pseudonimity of subscribers

AEGIS CA will neither issue nor 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

The subject name included in the CN part of a certificate must be unique for all certificates issued by the AEGIS CA. These certificates belong to the same end entity. When essential, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name.
Private keys must not be shared among end entities.
DNs cannot be recycled.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of a key

The AEGIS CA proves possession of the private key that is the companion to the public key in AEGIS CA root certificate by issuing certificates and signing CRLs.
The AEGIS CA 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 AEGIS CA 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

The AEGIS CA authenticates organizations by:

- Checking that organization is affiliated with AEGIS Initiative;
- Contacting the person who represents the organization in the project.

3.2.3 Authentication of individual entity

Certificate of a person:
The subject should contact personally the RA or CA staff in order to validate his/her identity. The subject authentication is fulfilled by providing an official document for personal identification (ID-card, driving license or a passport), and a valid document proving subject's relation with an institute or organization, declaring that the subject is a valid end entity.

Certificate of a host or service:
Host or service certificates can only be requested by the administrator responsible for the particular host. In order to request a host or service certificate the following conditions must be met:

1. The host must have a valid FQDN.
2. The administrator must already possess a valid personal AEGIS certificate.
3. The administrator must provide a proof of his or hers relation to the host itself.

The subscriber requesting service from the AEGIS CA must present valid documents for personal identification (ID-card, driving license or a passport), and a valid document proving subject's relation with an institute or organization.

AEGIS CA or RA will archive photocopies of ID documents in case of user certificates and digitally signed e-mails in case of host or service certificates.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of Authority

No stipulation.

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 personal certificate of the subscriber. Re-key after expiration uses completely the same authentication procedure as new certificate. For the first time and after that once every 3 years, a subscriber must be authenticated by the RA or CA serving his/her location following the procedure described in section 3.2.3.

3.3.2 Identification and authentication for re-key after revocation

The procedure for re-key after revocation 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 via a valid personal key corresponding to the certificate that is requested to be revoked which must be a valid, non-expired and non-revoked AEGIS certificate.
- For persons who do not have a valid AEGIS 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 by the RA should be done by e-mail, signed with 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 at least 1024 bits and the exponent must be greater than 3.
4. use a strong passphrase of at least 12 characters
5. **User certificate:** For the first time and after that once every 3 years, a subscriber must be authenticated by the RA or CA serving his/her location following the procedure described in section 3.2.3. The submission of the certificate requests will be done via an SSL secured web form or via e-mail. If the subscriber wants to re key his/her certificate, then he/she must follow the procedures described in section 4.7.
6. **Host or service certificate**: The subject must already have a valid AEGIS CA certificate before requesting a server or service certificate. The submission of the certificate request can be done either via a web interface or via e-mail. In the first case the subject will have first to import his/her AEGIS CA certificate in the browser in order to be authenticated automatically by the AEGIS CA or RA web interface. Upon successful authentication the user will be able to submit the certificate request via a SSL secured web based form or via digitally signed e-mail. In the second case the subject will have to send an e-mail signed with his/her AEGIS CA key to aegis-ca@aegis-ca.rcub.bg.ac.rs with the certificate requests attached and stating in the body of the e-mail that he is the person responsible for the server/service. In both cases the certificate request will be forwarded to the appropriate RA or CA, 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 AEGIS CA and RAs as stated in section 3.2.3. In the cases of re-key of user certificate or request for host or service certificate, the authentication of the certificate application will take place by checking that the requester has a valid AEGIS CA certificate. Upon successful authentication, the information included in the certificate request will be validated by RA or 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 or CA;
2. the subject must be an acceptable subscriber entity, as defined by this Policy (section 1.3.3);
3. the request must obey the AEGIS CA distinguished name scheme (section 7.1.4);

4. the distinguished name must be unique;
5. the key must be 1024 or 2048 bits;
6. each applicant generates his/her own key by using OpenSSL or similar software;
7. host and service certificate requests must be submitted via SSL secured web form or via e-mail signed by a valid AEGIS CA certificate;
8. user certificate requests must be submitted via SSL secured web form or via e-mail.
9. the requests for certification keys with exponent == 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 or CA to the requester with carbon copy to aegis-ca@aegis-ca.rcub.bg.ac.rs

4.2.3 Time to process certificate applications

Each certificate application will take no more that 3 working days to be processed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

If the certificate was requested through RA, the CA will validate the RA signature and RA authority and then issue the certificate.
If the user requested the certificate from the CA, the user must be validated as described in section 3.2.3 and then the certificate will be issued.
Right after the subscriber's certificate is issued, an e-mail will be sent to the relevant RA manager or to the subscriber informing him/her about the action.
Communication between CA and RA will be done via encrypted and digitally signed e-mails using S/MIME.

4.3.2 Notification to subscriber by the CA of issuance of certificate

If the RA handled the communication between Subscriber and CA, the RA will send an e-mail, informing about certificate issuance. If Subscriber contacted CA directly, the CA will send an e-mail, informing about certificate issuance. User can then download His or Her certificate from CA on-line repository.

4.4 Certificate acceptance

If the user wants to accept the certificate, he or she must follow the procedure in section 4.4.1.
If a user wants to reject a certificate, he or she must submit a revocation request as described in section 4.9.

4.4.1 Conduct constituting certificate acceptance

The subscriber must send an e-mail, within 5 working days from the day that his/her certificate was issued, in which he will be stating that:

1. He or She accepts his/her certificate signed by the AEGIS CA;
2. He or She assumes the responsibility to notify the AEGIS CA immediately:
   - in case of possible private key compromise;
   - when the certificate is no longer required;
   - when the information in the certificate becomes invalid.

The e-mail which the user sends to the CA has to be signed with the key corresponding to the public key in certificate he or she received from the CA.
If the subscriber does not send the e-mail within 5 working days, the certificate becomes the subject for revocation.

4.4.2 Publication of the certificate by the CA

All the certificates issued by the AEGIS CA will be published in the on-line repository operated by the AEGIS CA.

4.4.3 Notification of certificate issuance by the CA to other entities

If the RA has handled the communication with the subscriber, then it 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 keys along with the certificates issued by the AEGIS CA can be used for:

- email signing/verifying and encryption/decryption (S/MIME);
- server authentication and encryption of communications;
- authentication purposes in Grid Infrastructures.
    - non-repuditation

4.5.2 Relying party public key and certificate usage

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

- email encryption and signature verification (S/MIME);
- server authentication and encryption of communications;
- authentication purposes in Grid infrastructures.

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

AEGIS CA 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

See section 4.6.1.

4.6.3 Processing certificate renewal requests

See section 4.6.1.

4.6.4 Notification of new certificate issuance to subscriber

See section 4.6.1.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.6.1.

4.6.6 Publication of the renewal certificate by the CA

See section 4.6.1.

4.6.7 Notification of certificate issuance by the CA to other entities

See 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 AEGIS CA;
2. revocation of their certificate by the AEGIS CA;

4.7.2 Who may request certification of a new public key

Every subscriber holding a valid AEGIS CA certificate can request certificate re-key 1 day before expiration of the certificate.

4.7.3 Processing certificate re-keying requests

Expiration warnings will be sent to subscribers before it is re-key time.
a) Re-key before expiration can be executed by stating a re-key request signed with the private key corresponding to the public one in the valid personal certificate of the subscriber. The requester is not required to pass the authentication procedure described in section 3.2.3, if this does not contrast with c) or d).
b) Re-key after certificate expiration uses completely the same authentication procedure as that for the new certificate.
c) At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.
d) In case the request for a new certificate is due to revocation 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

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

- The CA is informed that the Subscriber has ceased to be a member of or associated with a AEGIS 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.

4.9.2 Who can request revocation

The CA, RA, 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 a valid AEGIS CA certificate. Otherwise authentication will be performed with the same procedure as 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

AEGIS CA will process all revocation requests within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Relying parts must download the CRL from the online-repository [section 2.1] 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 23 days;
2. The maximum CRL lifetime is 30 days;
3. Each new CRL is issued at least 7 days before expiration of the previous CRL.

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 AEGIS CA.

4.9.10 On-line revocation checking requirements

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

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

AEGIS CA does not suspend certificates.

4.9.14 Who can request suspension

AEGIS CA does not suspend certificates.

4.9.15 Procedure for suspension request

AEGIS CA does not suspend certificates.

4.9.16 Limits on suspension period

AEGIS CA does not suspend certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

AEGIS CA operates an on-line repository that contains all the certificates have been issued. The repository also contains CRL list. Promptly following revocation, the certificates and CRL 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

No stipulation.

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 AEGIS CA operates in a controlled and protected room located in University of Belgrade Computer Center. At least one person employed by Belgrade University Computer Center will always be present on premises 24 hours per day, 7 days per week.

5.1.2 Physical access

Physical access to the AEGIS CA is restricted to authorized personnel only.

5.1.3 Power and Air Conditioning

Premises containing the CA machine are air conditioned.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

University of Belgrade Computer Center premises have a fire alarm system installed.

5.1.6 Media storage

Backups are to be stored in removable storage media (CD-ROM, Floppies and USB Flash) in a safe location in University of Belgrade Computer Center premises.

5.1.7 Waste Disposal

Floppy disks or CDs 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

AEGIS CA personnel are selected in mutual agreement between AEGIS Coordinator and the respective AEGIS CA operating organization (University of Belgrade Computer Center).

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to AEGIS CA and RA operators.

5.3.4 Retraining frequency and requirements

AEGIS CA will perform operational audit of the CA/RA staff at least once per year. If the results of the operational audit are not satisfactory, retraining will 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 personnel during the initial training period.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events are recorded by AEGIS CA:

- 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 month.

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 CA 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 AEGIS CA.

5.4.7 Notification to event-causing subject

No stipulation.

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 CA:

- certification requests
- issued certificates
- requests for revocation
- issued CRLs
- all e-mail messages of correspondence between RA and CA
- identity validation records (section 3.2.3)

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.
- all e-mail messages of correspondence between RA and CA
- identity validation records (section 3.2.3)

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 AEGIS CA.

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Key changeover

The CA's 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 one year plus one month. 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 Computing resources, software, and/or data are corrupted

In case of signing machine, OS or AEGIS CA data files failure, AEGIS CA operation will be restored as fast as possible from latest backup.

5.7.2 Entity private key compromise procedures

If the CA's private key is (or is suspected to be) compromised, the CA 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;
- Make a new presentation of site security for CA re-accreditation.

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

5.7.3 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA Termination

Before the AEGIS CA terminates its services, it will:

- Inform the Registration Authorities, Subscribers and Relying Parties of which the CA is aware;
- Make information of its termination available on it's website;
- Stop issuing certificates.
- Annihilate all copies of private keys.
- Audit logs will be kept for 3 years from CA or RA termination date.

Before the AEGIS RA terminates its services, it will:

- Inform the CA and Relying Parties it is aware of.
- Make information of its termination available on it's and CA websites.
- 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 AEGIS CA root certificate are generated on a dedicated machine, not connected to any type of network. The software used for key generation is OpenSSL.
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, CA has no access to subscribers' private keys.

6.1.3 Public key delivery to certificate issuer

Applicants can make user/host/service certificate requests as described in section 4.1

6.1.4 CA public key delivery to relying parties

The AEGIS CA root certificate is available on the website: http://aegis-ca.rcub.bg.ac.rs/

6.1.5 Key Sizes

For a user or host certificate the key size is 1024 or 2048 bits. The AEGIS CA 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)

AEGIS CA Keys may be used for authentication, non-repudiation, data encipherment, key enicpherment, message integrity and session establishment.
AEGIS CA 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 AEGIS CA private key is kept encrypted in multiple copies in USB flash drive and CD-ROM in a safe location. The password for the private key is kept separately in paper form with an access control. Only authorized CA personnel have access to the backups.

6.2.5 Private key archival

AEGIS CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

AEGIS CA does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

AEGIS CA does not use any kind of cryptographic module.

6.2.8 Method of activating private key

The private key of the AEGIS 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

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

No stipulation.

6.3.1 Public Key Archival

As a part of the certificate archival, the public key is archived.

6.3.2 Certificate operational periods and key pair usage periods

AEGIS CA root certificate has a validity of ten years.
End Entity certificates have maximum lifetime of 1 year plus 1 month.

6.4 Activation Data

6.4.1 Activation data generation and installation

AEGIS CA does not generate activation data for subscribers. It's upon the subscriber to generate a secure pass phrase, at least 12 characters long, in order to be used as activation data for his/her private key.
AEGIS CA private key is protected by a passphrase of at least 15 characters. Pass phrase is regenerated every 180 days by one of AEGIS CA operators.

6.4.2 Activation data protection

The subscriber is responsible to protect the activation data for his/her private key.
The AEGIS CA uses a pass phrase to activate it's private key which is known only by the AEGIS CA Manager and the AEGIS CA Operators. A copy in written form of the pass phrase is sealed in an envelope and kept in a safe. Access to the safe is restricted only to the AEGIS CA Manager and Operators. 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 AEGIS CA meet the following requirements:

- 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

Only X.509 v3 certificates are issued by the AEGIS CA

7.1.2 Certificate Extensions

The values of extensions in case of CA certificate are following:

- X509v3 Basic Constraints: critical CA:TRUE
- X509v3 Key Usage: critical Certificate Sign, CRL Sign
- X509v3 Subject Key Identifier: <CA key ID>
- X509v3 Authority Key Identifier:
    - keyid:<CA key ID>
    - DirName:/C=RS/O=AEGIS/CN=AEGIS-CA
    - serial:<CA certificate serial>
- X509v3 Issuer Alternative Name: email:aegis-ca@aegis-ca.rcub.bg.ac.rs
- X509v3 Subject Alternative Name: email:aegis-ca@aegis-ca.rcub.bg.ac.rs
- X509v3 CRL Distribution Points
- Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA
- Netscape Comment: AEGIS Certification Authority Root Certificate

The values of extensions in case of user certificates are following:

- X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Non-Repuditation.
- 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>
    - DirName:/C=RS/O=AEGIS/CN=AEGIS-CA
    - serial:<CA certificate serial>
- X509v3 Subject Alternative Name: email:<user's email address>
- X509v3 Issuer Alternative Name: email:aegis-ca@aegis-ca.rcub.bg.ac.rs
- X509v3 Certificates Policies:
    - Policy: <OID of the effective CP/CPS>
- X509v3 CRL Distribution Points
- Netscape Cert Type: SSL Client, S/MIME, Object Signing
- Netscape Comment: AEGIS Certification Authority Policy: http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-CP-CPS.doc

The values of extensions in case of host and service certificates are following:

- X509v3 Basic Constraints: critical CA:FALSE

- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 Extended Key Usage: TLS Web Server Authentication
- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Authority Key Identifier:
  - keyid:<CA key ID>
  - DirName:/C=RS/O=AEGIS/CN=AEGIS-CA
  - serial:<CA certificate serial>
- X509v3 Issuer Alternative Name: email:aegis-ca@aegis-ca.rcub.bg.ac.rs
- X509v3 Subject Alternative Name: DNS:FDQN
- X509v3 Certificates Policies:
  - Policy: <OID of the effective CP/CPS>
- X509v3 CRL Distribution Points
- Netscape Cert Type: SSL Server
- Netscape Comment: AEGIS Certification Authority Policy: CP/CPS http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-CP-CPS.doc

Where XXX is the shortform of the name of the institution, the user or host/service are described in section 1.3. A current list of OU's can be obtained at http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-CP-CPS.doc

7.1.3 Algorithm Object Identifiers

The ODIs for algorithms used for signatures of certificates issued by AEGIS CA are according to:

- secure hash algorithm: sha-256 2.16.840.1.101.3.4.2.1
- encryption: rsaEncryption 1.2.840.113549.1.1.1
- signature: sha256WithRSAEncryption 1.2.840.113549.1.1.11

7.1.4 Name Forms

Issuer:
C=RS, O=AEGIS, CN=AEGIS-CA
Subject:
C=RS, O=AEGIS, OU=XXX, CN=Subject-name

Where XXX is the name or acronym of the institution. The "CN" field structure for the user or host/service are described in section 1.3. A current list of OU's can be obtained at http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-CP-CPS.doc

In case of person, the CN part of DN can contain only 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 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 128 characters for all types of certificates.

7.1.5 Name constraints

Subject attribute constraints:

Country:
Must be “RS”
Organization:
Must be “AEGIS”
OrganizationUnit:
Must be the name of the subject's institute.
CommonName:
First name and last name of the subject for user certificates, DNS FQDN for host or service certificates. In the latter case the DNS FQDN may be prefixed by the value 'host' or the service name separated with a '/' from the DNS FQDN.

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 version 2 format. This is indicated by setting the *version* field in CRL to value 1.

7.2.2 CRL and CRL entry extensions

The CRL extension Authority Key Identifier will be used in CRLs. CRL entry extensions used are: CRL Number and CRL Reason Code. They are described in the following sections.

7.2.2.1 Authority key identifier

Non-critical extension, a unique identifier for the CA key as defined in RFC 3280.

7.2.2.2 CRL Number

Non-critical extension, the number of current CRL as defined in RFC 3280.

7.2.2.3 CRL Reason Code

Non-critical extension, carrying the revocation reason code as specified in RFC3280, section 5.3.1.

7.3 OCSP profile

No stipulation.

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 AEGIS CA must allow to 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.

Any changes made to the CP/CPS document must be approved by the responsible PMA prior of signing any certificates under the new CP/CPS version.

Users will not be informed in advance of changes to AEGIS CA's CP/CPS.

AEGIS CA will perform operational audits of the RA staff, at least once per year. A list of CA and RA personnel will be maintained and verified at least once a year.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

Auditors should be independent of the AEGIS.

8.4 Topics covered by assessment

Auditors will conduct the compliance audits according to EUGridPMA recommendations.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

Within 30 days of receiving compliance audits, the AEGIS CA will prepare a statement regarding the issues, and if necessary, present a new CP/CPS.

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

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

9.2 Financial responsibility

AEGIS CA denies any financial responsibilities for damages or impairments resulting from its operation.9.2.1 Insurance coverage

9.2.1 Insurance coverage

No stipulation

9.2.2 Other assets

No stipulation

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation

9.3.2 Information not within the scope of confidential information

No stipulation

9.3.3 responsibility to protect confidential information

No stipulation

9.4 Privacy of personal information

AEGIS CA does not collect any confidential or private information.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

AEGIS CA collects the following information which is not deemed as private:

1. subscriber's e-mail address;
2. subscriber's name;
3. subscriber's organization;
4. subscriber's certificate;

9.4.4 Responsibility to protect private information

AEGIS CA has not responsibility to protect private information as all the information it collects is public.

9.4.5 Notice and consent to use private information

AEGIS CA and RA's will only use private information if a subscriber has given full consent in the course of the registration process. All collected information will be subject to the Serbian law.

9.4.6 Disclosure pursuant to judicial or administrative process

AEGIS CA will release private information on judicial or other authoritative order.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

1. RFC 3647;
2. HellasGrid CA Certificate Policy;
3. TR-Grid CA Certificate Policy;
4. UK e-Science CA Certificate Policy;
5. SEE-GRID CA Certificate Policy;

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

1. AEGIS CA guarantees to control the identity of the certification requests according to the procedures described in this document;
2. AEGIS CA guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. AEGIS CA is run on a best effort basis.
4. AEGIS CA guarantees its service security.
5. AEGIS CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates ;
6. AEGIS 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

Amendments to this document must be approved by the EUGridPMA. Rephrasing to improve understandability as well as minor corrections are not considered amendments.

9.12.2 Notification mechanism and period

The amended document will be published on the AEGIS CA website at least one week before becoming active.

9.12.3 Circumstances under which OID must be changed

Substantial changes will cause the OID to be changed. The decision is made by the AEGIS CA manager and submitted to the EUGridPMA for approval.

9.13 Dispute resolution provisions

Legal disputes arising from the operation of the AEGIS CA will be resolved according to the Serbian Law.

9.14 Governing law

The enforceability, construction, interpretation, and validity of this policy shall be governed by the Laws of Serbia.

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.

The CP/CPS document and all CPS modifications should be approved by the EuGridPMA before being applied.