Certification Authority
IRAN-GRID CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Document OID: 1.3.6.1.4.1. 32426.1.1.2.0.0

Version 2.0
March 18, 2009

Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran.
P. O. Box 19395-5746
Tel: + 98 21 2228 8680
Fax: + 98 21 2229 0151
URL: http://www.ipm.ac.ir

1. INTRODUCTION

This document is structured according to RFC 3647 [RFC3647]. Not all sections of RFC 3647 are used. Sections that are not included have a default value of "No stipulation". This document describes the set of rules and procedures established by IPM (Institute for Studies in Theoretical Physics and Mathematics) for the operations of the Iranian Grid Certification Authority (IRAN-GRID CA) service. The data center housing the IRAN-GRID CA server is located in Tehran. This document will include both the Certificate Policy and the Certification Practice Statement for the IRAN-GRID CA. The general architecture is a single certification authority and several registration authorities.

1.1 OVERVIEW

IRAN-GRID CA is the infrastructure to support e-science activities provided by the IPM . This document describes the set of rules and operational practices that shall be used by the IRAN-GRID CA, the Certification Authority (CA), for issuing certificates. This and any subsequent CP/CPS document can be found on its web site http://cagrid.ipm.ac.ir.

1.2 DOCUMENT NAME AND IDENTIFICATION

Title: IRAN-GRID CA Certificate Policy and Certification Practice Statement
Version: 2.0
Date: 18th March 2009
Approved: proposed to be approved
Expiration: This document is valid until further notice.
ASN.1 OID: 1.3.6.1.4.1. 32426.1.1.2.0

IRAN-GRID CA Institute for Studies in Theoretical Physics and Mathematics (IPM)	1.3.6.1.4.1. 32426
Grid Computing Group (GCG)	1
CP/CPS	1
Major Version	2

Minor Version	0

1.3 PKI PARTICIPANTS

The IRAN-GRID CA issues certificates to the Iranian academic and research communities and other related entities for e-Science and Grid computing related activities.

1.3.1 CERTIFICATION AUTHORITIES

The certification authority is a stand-alone self-signed CA. The IRAN-GRID CA does not issue certificates to subordinate Certification Authorities.
All certificates will only be issued based on approved versions of the CP/CPS by EUGridPMA and must be signed by the IRAN-GRID CA.

1.3.2 REGISTRATION AUTHORITIES

Registration Authorities (RAs) of IRAN-GRID CA perform authentication of certificate requesters on behalf of IRAN-GRID CA. Currently, there is only one RA, IRAN-GRID CA itself. New registration authorities may be created by the IRAN-GRID CA as required, and will Be updated to the list of active RAs: http://cagrid.ipm.ac.ir/ra.htm.

1.3.3 SUBSCRIBERS (END ENTITIES)

The IRAN-GRID CA issues certificates for e-Science activities performed within the Iranian grid computing community. The CA will issue personal, server and service certificates for entities related with the following organizations:

a) Iranian academic organizations (e.g. public and private universities and educational institutes);
b) Iranian academic research centers (either public or private, non-profit ones); and,
c) Other organizations with research and development (R&D) affiliations with one of the above classes of organization.

The subject entities for certificates are of the following types:

a) Employees, researchers and students related with the above organizations; or,
b) Computer systems and services related with the above organizations;

All subjects will be uniquely identified for the entire lifetime of the IRAN-GRID CA, not just the period of validity of the certificate.

1.3.4 RELYING PARTIES

Relying parties are individuals or organization using the certificate issued by IRAN-GRID CA to verify the identity of subscribers and to secure communication with these subscribers.

1.3.5 OTHER PARTICIPANTS

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The certificates issued by IRAN-GRID CA may be used for any application that is suitable for X.509 certificates, in particular:

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

They may only be used or accepted for actions compatible with the certificate extensions.

1.4.2 PROHIBITED CERTIFICATE USES

Certificates issued by the IRAN-GRID CA are only valid in the context of the scientific-academic Grid activities in Iran. Any other usages such as financial transactions or classified projects are strictly forbidden.

They must not be used for purposes that violate Iranian law or the law of the country in which the target entity (i.e. application or host to use, addressee of an e-mail) is located.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The IRAN-GRID Certification Authority is responsible for the registration, maintenance, and interpretation of this CP/CPS. This CA is managed by the Grid Computing Group (GCG) at the Institute for studies in Theoretical Physics and Mathematics(IPM), located in Tehran (Iran). The full IRAN-GRID CA postal address for operational issues is:

Grid Computing Group (GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM)

Niavaran Bldg., Niavaran Sqr.,Tehran,Iran.

Phone: (+98 - 21) 22288680

Fax: (+ 98 -21) 22280415

Email: ca-manager@ipm.ir

1.5.2 CONTACT PERSON

The contact person for questions related to this document or any other issues related to the IRAN-GRID CA is the current CA manager:

Majid Arabgol

Grid Computing Group(GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM), Opposite the ARAJ, Artesh Highway, Tehran, Iran
P.O.Box: 19395-5531
Tel: +98 (21) 26 13 06 76
Fax: +98 (21) 22 80 91 48
Email: arabgol@ipm.ir

1.5.3 Person determining CPS suitability for the policy

Shahin Rouhani

Head, Grid Computing Group(GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM), Opposite the ARAJ, Artesh Highway, Tehran, Iran
P.O.Box: 19395-5531
Tel: +98 (21) 26 13 06 76
Fax: +98 (21) 22 80 91 48
Email: rouhani@ipm.ir

1.5.4 CPS approval procedures

Each version of this document shall be submitted to EUGridPMA for approval and accreditation.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

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 [RFC2119].

Activation Data
Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (i.e., a PIN, a passphrase, or a manually-held key share).

Authentication
The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization which applies for or seeks access to something under a certain name is, in fact, the proper individual or organization. This process corresponds to the second process involved with identification, as shown in the definition of "identification"

below. Authentication can also refer to a security service providing assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

Certification Authority (CA)
An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole lifetime. That entity / system issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA)

Certificate Policy (CP)
A named set of rules indicating the applicability of a certificate to a particular community and/or class of applications with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions.

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

Community RM
One or more RMs that serve multiple, low request rate, sites / Virtual Organizations.

Host Certificate
A Certificate for server certification and encryption of communications (SSL/TSL). It represents a single machine.

Identification
The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named.

Individual or Organization.
A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (Issuing CA)
In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Person Certificate
A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Qualifier
The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Point of Contact
The member of a site/VO RA that has been chosen to handle all communications about policy matters with the Grid manager.

Private RM
RMs that serve high certificate request rate sites / Virtual Organizations, and that are operated by the site/VO.
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 a CA).
Registration Agent (RAg) or "Agent"
RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.
Registration Manager (RM)
The RM is a front-end Web server for the CA that provides a Web user interface for CA subscribers and agents. The RM forwards certificate signing requests to the actual CA to issue X.509 certificates.

Relying Party (RP)
A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Repository
A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.

Service Certificate
A certificate for a particular service running on a host. It will represent a single service on a single host.
Host certificate

A certificate used for server authentication and encryption of communications. It will represent a single machine.
Subscriber
Or sometimes called End Entity is a person who a digital certificate is issued.

Virtual Organization (VO)
An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at. (i.e. PPDG, FNC, EDG, etc).

SHA1
SHA stands for **S**ecure **H**ash **A**lgorithm. Hash algorithm complete a fixed-length digital representation (known as a message digest)of an input data sequence (the message) of any length. They are called "secure" when, "it is computationally infeasible to:

- Find a message that corresponds to given message digest, or
- Find two different messages that produce the same digest.

SHA1 is a superior version of its implementation i.e. SHA0. It was considered to be the successor to MD5 (Message Digest%), an earlier , widely hash function.

SSL
Secure **S**ocket **L**ayer is a protocol that transmits our communications over the network in an encrypt form and ensures that information is sent unchanged, only the computer we intended to send it to.

1.6.2 ACRONYMS

C	Country
CA	Certification Authority
CN	Common Name
CDROM	Compact Disc Read Only Memory
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished name
EUGridPMA	The European Grid Authentication Policy Management Authority in e-Science, http://www.eugridpma.org/
IRAN-GRID CA	Iranian Grid Certificate Authority for e-sciences
IPM	Institute for studies in Theoretical Physics and Mathematics
LDAP	Lightweight Directory Access Protocol
MIME	Multi-purpose Internet Mail Extensions
NTP	Network Time Protocol
O	Organization
OU	Organizational Unit
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Sockets Layer
URI	Universal Resource Identifier
URL	Universal Resource Locator
OID	Object Identifier
FQDN	Fully Qualified Doman Name

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The online repository of information from the IRAN-GRIFD CA is accessible at the URL: http://cagrid.ipm.ac.ir

2.2 PUBLICATION OF CA INFORMATION

The IRAN-GRID CA will operate a secure online repository that contains:

1. IRAN-GRID CA root certificate in PEM, DER, CRT, CER and text formats.
2. Freshest CRL in PEM, DER and text formats.
3. A copy of the recent version of IRAN-GRID CA CP/CPS and all previous versions.
4. User, host and service certificates issued by IRAN-GRID CA.
5. Contact addresses including physical address and email address.
6. List of its RAs.
7. List of organizations, whose employees are eligible for requesting certificates from IRAN-GRID CA (Authenticated Organizations).
8. Other information that can be regarded as relevant to IRAN-GRID CA

2.3 TIME OR FREQUENCY OF PUBLICATION

All information published shall be up-to-date.
Certificates will be published to the IRAN-GRID CA repository as soon as issued.
The certificate revocation list (CRL) shall have a lifetime of at most 30 days. The IRAN-GRID CA must issue a new CRL at least 7 days before expiration or immediately after having processed a revocation, whichever comes first. A new CRL must be published immediately after its issuance.

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

2.4 ACCESS CONTROL ON REPOSITORIES

The online repository is maintained on a best effort basis and is available substantially on 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance. Outside the period 08:30-16:30 (local time - GMT) Monday-Friday it may run unattended. The IRAN-GRID CA does not impose any access control on its CP/CPS, its certificate, 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 the case of user certificates the subject name must include the person's name in the CN field;
2. In the case of host certificates the subject name must include the DNS FQDN in the CN field;
3. In the case of service certificates the subject name must include the service name and the DNS FQDN separated by a '/' in the CN field.

Any name under this CP/CPS is in the form of "C=IR, O=IRAN-GRID, O=string, OU=string". The following part is the "CN" which is distinguished for each person, each host or each service.

Illustration of a full subject distinguished name for a user:
C=IR, O=IRAN-GRID, O=Sharif University of Technology, OU=Physics Dept. , CN= Shahin Rouhani (Full Name)
Illustration of a full subject distinguished name for a host:
C=IR, O=IRAN-GRID, O= Sharif University of Technology OU= Physics Dept. , CN=grid02.sharif.ac.ir
Illustration of a full subject distinguished name for a service:
C=IR, O=IRAN-GRID,O=Sharif University of Technology , OU= Physics Dept, CN=ldap/grid02.sharif.ac.ir
The common names must be encoded as Printable Strings according with RFC 1778 [RFC1778] and RFC 2252 [RFC2252]. The characters allowed in the common names of personal certificates are as follows:

1. ' ' (space), '(', ')' and '-';
2. '0' – '9';
3. 'a' – 'z' and 'A' – 'Z'.

In addition, the characters '.' (period) and '/' (slash) are allowed in host and service certificates. The period must be used to separate the DNS host name components and the slash must be used to separate the service name or the keyword "host" from the DNS host name.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber. Subscribers must choose a representation of their names in the permitted character set (see 3.1.1). The name must not refer to a role. Subscribers can neither be anonymous nor pseudonymous.

3. 1.3 ANONYMITY OR PSEUDONIMITY OF SUBSCRIBERS

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

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

See section 3.1.1.

3.1.5 UNIQUENESS OF NAMES

The Distinguished Name must be unique for each end entity certified by the IRAN-GRID CA service. The IRAN-GRID checks uniqueness before approving the request.
In this policy two names are considered identical if they differ only in case. In other words, case must not be used to distinguish names.
If necessary, additional numbers or letters are appended to the common name to guarantee the uniqueness of the subject name.
Name uniqueness is preserved for the lifetime of the CA Certificates must apply to unique individuals or resources. Subscribers must not share certificates.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

Possession of the private key is verified for certificate issued by the IRAN-GRID CA through the verification of the digital signature on the certificate signing request (CSR) as the registered user always generates his own key pair when requesting a certificate.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

- If an organization wishes to establish an RA they must contact the CA. The CA verifies the eligibility of the organization.
- An organization/unit that wants to get a certificate for a natural person, a server or a service, has to announce this officially to the appropriate RA. The RA has to as certain that the organization or organizational unit exists and is entitled (see 1.3.3) to request a IRAN-GRID certificate.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

In order to enable the RA to authenticate the individual's identity the latter must meet in person with the RA (face to face) and present an officially recognized document proving the requesting party's identity. Only documents accepted by Iranian law (Iranian national identity card or passport) will be accepted.
For each authentication, the RA will record and archive:

- The type, identification number and name in the identification document presented by the subject to be authenticated;
- A contact e-mail, phone number and address of the requester;
- The identification of the person that has performed the authentication;
- The date, time and place of the authentication;

For host or service certificates, the requests must be signed with a IRAN-GRID CA issued personal certificate corresponding to the system administrator or person responsible of the resource. The RA corresponding to the organization mentioned in the certificate request distinguish name will verify whether the requester has the right to request a

certificate for the intended host or service and that the FQDN has been registered in the Internet's DNS.
The RA shall send in a signed e-mail to the IRAN-GRID CA, an electronic copy of the recorded authentication documentation and the certificate request. The information will be stored in a secure database at the CA site and shall be considered private and confidential (see 9.4).

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

No stipulation.

3.2.5 VALIDATION OF AUTHORITY

Any organization or unit willing to host an RA for IARN-GRID certificates shall appoint one or more representatives who are entitled to request server or service/application certificates and answer all questions related to natural-person certificate requests.
These representatives shall be the first in their organization/unit to request individual certificates according to the provisions outlined in 3.2.3. The signatures of these individuals with the private key associated with the certified public key shall be sufficient for all future information exchanges with or requests from that organization/unit.
When the organization/unit rescinds the individual's authorization it has to inform the RA and the IRAN-GRID CA in the same way as it has made the authorization known.

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 the certificate expires can be done using a secure web interface or by sending a re-key request based on a new public key in an e-mail signed with old private key to the appropriate RA of the IRAN-GRID CA. After expiration of the certificate no re-key is possible; a new application for initial registration must be made instead.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

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

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

In case of emergency the revocation can be initiated via oral communication with the appropriate RA or the IRAN-GRID CA. The RA or the IRAN-GRID CA have to use their best effort to authenticate the request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

The IRAN-GRID CA issues certificates to subscribers from authenticated organizations (see 1.3.3) for:

- natural persons,
- hosts administered by the requesting organization:
    - hosts belonging to the member organization
    - hosts under the member organization responsibility
- Services provided on a host that is administered by an eligible organization.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

The requesting party generates the key pair with a size of at least 1024 bits on their system through the form provided at the IRAN-GRID CA web site. After the form has been completed the encrypted private key will be stored on the system where the browser runs, in a file only accessible to the requester (if the operating system allows such a restriction).

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

For the natural persons the RA operator must authenticate the individual's identity (see 3.2.3). In the case of a server/service request it must also check that the user is a representative (see 3.2.5) of the organization or unit responsible for the host.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

Upon successful authentication, an electronic copy (signed by the RA) of the certification request shall be sent to the IRAN-GRID CA. Alternatively, a secure transmission to the IRAN-GRID CA may be used, if it is at least as secure as a signed e-mail.
The necessary provisions that must be followed in any certificate application request to the IRAN-GRID CA are in order to be approved:

1. The certificate request must be submitted by the user via an online procedure.
2. The certificate application must be authenticated by the RA as described in section 4.2.1;
3. The subject must be an acceptable subscriber entity, as defined by this Policy;

4. The request must obey the IRAN-GRID CA distinguished name scheme;
5. The distinguished name must be unambiguous and unique;
6. The key must have at least 1024 bits.

If the certificate request does not meet one or more of the above criteria, it will be rejected and signed notification e-mail will be sent by the RA to the subject with carbon copy to ca-manager@ipm.ir

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

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

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

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

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The IRAN-GRID system shall then send an email to the requesting party with the URL of the certificate download page. It shall also send an acknowledgment of the issuance to the appropriate RA.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The requesting party shall notify the IRAN-GRID CA of the rejection of a certificate, explaining the IRAN-GRID CA and the RA the reasons for the rejection. Certificates whose rejection have not been received by the IRAN-GRID CA within a week shall be considered accepted.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The IRAN-GRID CA will publish on its web server certificates as soon as they are issued.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The RA that has handled communication with the subscriber will be notified of the certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Certificates issued by the IRAN-GRID CA and their associated private keys must only be used according to the permissions and prohibitions stated in section 1.4. They must only be

used according to the key usage fields of the certificate. When a certificate is revoked or expired the associated private key shall not be used anymore.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

A relying party must, upon being presented with a certificate issued by the IRAN-GRID CA
Check

- Its validity by
    - Verifying that the certificate is issued by IRAN-GRID CA ,
    - Checking that the certificate hasn't expired,
    - Consulting the IRAN-GRID CA CRL in effect at the time of use of the certificate.
- That the intended use of the certificate is appropriate as indicated by the key usage fields in the certificate and as specified in the CP pointed to by the certificate.

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

IRAN-GRID CA will not renew subscriber's certificate. 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 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

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

the certificate's parameters. The IRAN-GRID CA does not perform a re-key of a certificate after its revocation. A new certificate must be requested and the procedure for obtaining a new certificate must be followed.

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

Expiration warnings will be issued to subscribers 30 days before re-key time arrives. Re-key before expiration can be accomplished using a secure web interface or by sending a re-key request signed with the current user certificate (see 3.3.1). Re-key after expiration follows the same authentication procedure as for a new certificate. At least once every 5 years the subscriber must go through the same authentication procedure as the one described for a new certificate.
In case the request for a new certificate is due to revocation or compromise of certificate the subscriber must follow the same procedure as the one described in for a new one.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Same as in section 4.3.2

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Same as in section 4.4.1

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Same as in section 4.4.2

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Same as in section 4.4.3

4.8 CERTIFICATE MODIFICATION

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Certificates must not be modified. The old certificate must be revoked, and a new key pair must be generated and a request for the modified certificate contents must be submitted with the new public key.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Not applicable.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Not applicable.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not applicable.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE
Not applicable.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA
Not applicable.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES
Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 CIRCUMSTANCES FOR REVOCATION
A certificate will be revoked in the following circumstances:

1. The subject of the certificate has ceased being an eligible end entity for certification, as described in this policy;
2. The subject does not require the certificate anymore;
3. The private key has been lost or compromised;
4. The information in the certificate is wrong or inaccurate;
5. The system to which the certificate has been issued has been retired;
6. The subject has failed to comply with the rules of this policy.

4.9.2 WHO CAN REQUEST REVOCATION?
A certificate revocation can be requested by:

1. The owner of the certified key
2. The IRAN-GRID CA or any RA that has proof of a compromise
3. The organization that wants to revoke its consent to its inclusion in the certificate
4. The Registration Authority which authenticated the holder of the certificate;
5. The holder of the private key;
6. Any person presenting proof that the any one of the circumstances in section 4.9.1 is fulfilled.

4.9.3 PROCEDURE FOR REVOCATION REQUEST
Unless the IRAN-GRID CA acts on its own a revocation request must be made by:

1. The owner of the certificate, properly authenticated, using the online revocation facilities. In case of emergency (key compromise), the owner of the certificate must go to the RA as soon as possible and ask the appropriate RA to request revocation.
   Or
2. The RA administrator using a secure web interface

4.9.4 REVOCATION REQUEST GRACE PERIOD
There is no grace period defined for a revocation request. The IRAN-GRID CA shall process the authenticated request with priority and publish the revocation as fast as possible.

4.9.5 Time within which CA must process the revocation request
The IRAN-GRID CA must process all revocation requests without delay within 1 working day.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES
Before using a certificate the relying party must validate it against the CRL most recently published in the IRAN-GRID CA repository.

4.9.7 CRL ISSUANCE FREQUENCY
A new CRL is published in the on-line repository after every certificate revocation and at least 7 days before the expiration of the current CRL.

4.9.8 MAXIMUM LATENCY FOR CRLS
The CRL shall be copied to a removable device immediately after creation on the offline CA system and transferred without delay to the on-line repository.

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
IRAN-GRID CA does not suspend certificates.

4.9.14 WHO CAN REQUEST SUSPENSION
See section 4.9.13.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST
See section 4.9.13.

4.9.16 LIMITS ON SUSPENSION PERIOD
See section 4.9.13.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS
See section 2.2.

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
The subscription ends with the expiry of the certificate if it is not rekeyed before that date. A subscription may end earlier if the subscriber requests a revocation of its certificate.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES
No key escrow or recovery services are provided. The key owner must take all steps to prevent a loss.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES
See Section 4.12.1.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS
The IRAN-GRID CA is located at the Grid computing Group (GCG) of the IPM in Tehran. The IRAN-GRID CA is offline at all times and in a safe-fire box when not in use. IRAN-GRID maintains a limited access procedure to the system. All accesses to the server are limited to the IRAN-GRID staff.

The IRAN-GRID CA is run on Linux system (Fedora Core 7).

5.1.1 SITE LOCATION AND CONSTRUCTION
The IRAN-GRID CA is located at the following address:

Grid Computing Group(GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM), Opposite the ARAJ, Artesh Highway, Tehran, Iran

P.O.Box: 19395-5531
Tel: +98 (21) 26 13 06 76
Fax: +98 (21) 22 80 91 48

5.1.2 PHYSICAL ACCESS

The CA operates in a controlled environment, where access is restricted to authorized people. The machine hosting the CA (also known as the signing machine) and the private key are kept locked in a safe when not used.

5.1.3 POWER AND AIR CONDITIONING

The online machine operates in an air conditioned environment and is not rebooted or power-cycled except for essential maintenance.
The signing machine is switched off between signing operations and operates in an air conditioned environment.
The IRAN-GRID CA signing machine and the online machine are both protected by uninterruptible power supplies during their operations.

5.1.4 WATER EXPOSURES

Due to the location of the IRAN-GRID CA facilities, floods are not expected.

5.1.5 FIRE PREVENTION AND PROTECTION

IRAN-GRID CA facilities adhere to the Iranian law regarding fire prevention and protection in public buildings.

5.1.6 MEDIA STORAGE

Several copies of the IRAN-GRID CA private key are kept on removable storage media of different types (USB-HD, flash and CD-ROM) in secure location.

5.1.7 WASTE DISPOSAL

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

5.1.8 OFF-SITE BACKUP

No off-site backups are currently performed.

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 stipulations.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

No stipulations.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

All IRAN-GRID CA personnel must be suitably trained persons who are familiar with the PKI infrastructure and operation, and who possess the relevant technical and professional competence.

5.3.2 BACKGROUND CHECK PROCEDURES

- All access to the servers and applications that comprise the IRAN-GRID service is limited to IRAN-GRID staff.
- The RA Manager must be an employee of the Physical Organization hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that physical organization. The RA Manager has to be a member of that Department. The Registration Authority will make a declaration to the CA Manager in writing on the organization's headed note paper. The information that must be contained in this letter is defined by the CA Manager.
- The RA Operator must be an employee of the site hosting that Registration Authority and will be appointed by the RA Manager concerned. The RA Manager will make a declaration to the CA Manager in writing on the organization's headed note paper. If the RA Operator is appointed in a different department from the RA Manager then the letter must be countersigned by an authority for the department in which the Operator is appointed. The information that must be contained in this letter is defined by the CA Manager. RA Operators must have certificates and must adhere also to the subscriber's obligations.
- An RA Manager may appoint himself/herself as an RA Operator.
- An RA Manager may appoint any number of RA Operators.

5.3.3 TRAINING REQUIREMENTS

Internal training is given to IRAN-GRID CA/RA operators

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

In the event of unauthorized actions, abuse of authority or unauthorized use of entity systems by the CA or RA Operators, the CA manager may revoke the privileges concerned. The IRAN-GRID CA also reserves the right to prosecute unauthorized actions to the fullest extent under the legal provisions of the appropriate organization and Iranian law.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

No stipulation.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

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

- It is the responsibility of the CA Manager to provide the CA Operators with a copy of the "IRAN-GRID CA Operator's Procedure".
- It is the responsibility of the CA Manager to provide the RA Manager with a copy of the "IRAN-GRID RA Manager's Procedure".
- It is the responsibility of the CA Manager to provide the RA Operator with a copy of the "IRAN-GRID RA Operator's Procedure".

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

The following events shall be recorded:

- IRAN-GRID CA host
    - login / logout / reboot
    - issued signed certificates
    - creation and signing of certificates
    - revocation of certificates
    - CRL issues
    - audit log events
- IRAN-GRID web online server
    - login / logout / reboot
    - receipt of certificate request
    - issued certificates
    - receipt of certificate revocation request
    - validation of certificate request from online server
    - export of CSRs from online server
    - revocation of certificate
    - deleted certificate request
    - CRL issues

5.4.2 FREQUENCY OF PROCESSING LOG

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

5.4.3 RETENTION PERIOD FOR AUDIT LOG

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

5.4.4 PROTECTION OF AUDIT LOG
The audit logs shall only be accessible to the IRAN-GRID CA operators and managers.

5.4.5 AUDIT LOG BACKUP PROCEDURES
The audit logs shall be backed-up on a removable medium ,and kept a safe storage in a room with limited access.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)
The audit log accumulation system is internal to the IRAN-GRID CA.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT
Not defined

5.4.8 VULNERABILITY ASSESSMENTS
Not defined

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED
Following data will be recorded:

- All events defined in section 5.4.1.
- Identity validation records which RA collects, defined in section 3.2.3.

5.5.2 RETENTION PERIOD FOR ARCHIVE
The minimum retention period is 3 years.

5.5.3 PROTECTION OF ARCHIVE
The archive shall only be accessible to the IRAN-GRID CA operation, to management personnel and to authorized external auditors (see Section 8.3)

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

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS
All event records shall bear a time-stamp.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)
The archive collection system is internal to the IRAN-GRID CA.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION
All certificate data published by IRAN-GRID CA are publicly available. Data used for the registration and identification of subscribers are for internal use only. The integrity of IRAN-GRID CA archives is verified:

- At the time the archive is prepared
- At the time of a programmed security audit
- At any other time when a full security audit is required.

5.6 KEY CHANGEOVER

In the case of a changeover of the IRAN-GRID CA's key pair, an overlap of the old and new keys will exist. While the new key will be used for signing certificate, the older but still valid certificate must be available to verify old digital signatures – and the private key to sign CRLs – until all the certificates signed using the associated private key have also expired. The overlap of the old and new key must therefore be at least as long as the validity of an end entity certificate (see 6.3.2).

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If the private key of an end entity is lost or compromised due to corruption, the end entity must inform their RA immediately in order to request the revocation of their certificate. All relying parties known to accept the key should be informed by the owner of the key.
If the private key of the IRAN-GRID CA is (or is suspected to be) compromised, the CA Manager must:

- Make every reasonable effort to notify subscribers and RAs;
- Terminate the issuing and distribution of certificates and CRLs;
- Request revocation of the compromised certificate;
- Generate a new CA key pair and certificate and publish the certificate in the repository;
- Revoke all of the valid certificates that have been previously signed by the compromised key;
- Publish the new CRL on the IRAN-GRID CA repository;
- Notify relevant security contacts; and
- Notify relying parties and peer CAs, of which the CA is aware, as widely as possible.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

The CA will take best effort precautions to enable recovery.
In order to be able to resume operation as fast as possible after the compute basis of the CA is corrupted, the following steps shall be performed:

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

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

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

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The IRAN-GRID CA is located inside a building that is part of governmental facilities for research and higher education. The plans for business continuity and disaster recovery for governmental activities related to research and education are applicable.

5.8 CA OR RA TERMINATION

Before IRAN-GRID CA terminates its services, it will:

- Inform the Registration Authorities, subscribers and relying parties the CA is aware;
- Inform the EUGridPMA;
- Make information of its termination widely available;
- Stop issuing certificates
- Revoke all certificates
- Issue an publish CRL
- Destroy its private keys and all copies

An advance notice of no less than 60 days will be given in the case of normal (scheduled) termination. The CA Manager at the time of termination shall be responsible for the subsequent archival of all records as required in section 5.5.2.
The CA Manager may decide to let the CA issue CRLs only during the last year (i.e. the maximal lifetime of a subscriber certificate) before the actual termination; this will allow subscribers' certificates to be used until they expire. In that case notice of termination is given no less than one year and 60 days prior to the actual termination, i.e. no less than 60 days before the CA ceases to issue new certificates.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

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

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

Each subscriber must generate his/her own key pair using the IRAN-GRID CA web interface.
The CA does not generate private keys for its subscribers.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Subscribers public keys are delivered to the issuing CA by the SSL protected HTTP protocol via the IRAN-GRID CA web interface.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The CA certificate (containing its public key) is delivered to subscribers by online transaction from the IRAN-GRID CA online web server. It can be downloaded from the repository (see 2.1).

6.1.5 KEY SIZES

RSA Keys with a modulus of less than 1024 bits are not accepted. The IRAN-GRID CA key is of length 2048 bits.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Not defined.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

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

- With an end-entity certificate for
    - Authentication
    - key encipherment
    - message integrity
    - session establishment

- With the self-signed CA certificate
    - certificate signing
    - CRL signing
    - Certificate revocation

The CA's private key is the only key that can be used for signing certificates and CRLs.

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

Private keys must not be escrowed

6.2.4 PRIVATE KEY BACKUP

An extra instance of the private key encrypted with a randomly generated passphrase of at least 15 characters shall be stored on removable media which must be deposited in a safe and locked up place; the passphrase shall be stored on a different removable media or written down, and the media or paper shall be placed in a sealed envelope and stored in a secure place.
No instance of the private CA key (plain or encrypted) shall reside on the permanent disc of any computer that is online.

6.2.5 PRIVATE KEY ARCHIVAL

No stipulation.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

No stipulation.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

No stipulation.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

The CA private key is activated by providing the passphrase.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

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

6.2.10 METHOD OF DESTROYING PRIVATE KEY

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

6.2.11 CRYPTOGRAPHIC MODULE RATING

No stipulation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

The CA archives all issued certificates on removable media that is stored offline in a secure vault.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The validity of the certificate issued by the IRAN-GRID CA is defined by this CP/CPS document.
Subscriber's certificates have a validity period of one year plus 30 days, or less if the affiliation of the requesting party to the group participating in IRAN-GRID is less than one year.
The CA certificate has a validity period of 5 years.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

Each private key are protected by a strong passphrase consisting of at least 12 characters.

6.4.2 ACTIVATION DATA PROTECTION

All IRAN-GRID CA Operators know the activation data for the CA private key. No other person knows the activation data. However, activation data for the CA private keys is also kept in a sealed envelope in a safe. Access to the safe is restricted only to the authorized personnel.
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

Not defined.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The server hosting the CA product is run on a Linux system (Fedora Core).
No other services or software are loaded or operated on the CA server. The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of IRAN-GRID staff.

6.5.2 COMPUTER SECURITY RATING

Not defined.

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 signing machine will never be connected to a computer network under any circumstances. Certificates are generated on a machine not connected to any kind of network, located in a secure environment and managed by a suitably trained person. The public machine is protected by a suitably configured firewall.

6.8 TIME-STAMPING

All time stamping of entries created on the online servers at the IRAN-GRID CA is based on the network time provided by the time server of Fedora , synchronized with the official providers of time signals.

The hardware clock of the offline system for the certificate and CRL signing, which determines the time stamping of the certificates and the CRLs, will be synchronized manually by the operator whenever the host starts.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

All certificates issued by the IRAN-GRID CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280 [RFC3280].

7.1.1 VERSION NUMBER(S)

Only X.509 version 3 certificates are issued by the IRAN-GRID CA.

7.1.2 CERTIFICATE EXTENSIONS

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

For natural person certificates:

Basic Constraints:	critical, ca: false
Subject Key Identifier:	hash
Authority Key Identifier:	keyid
Key Usage:	critical,digitalSignature,keyEnciphermnet,dataEncipherment
Extended Key Usage	clientAuth,emailProtection
CRL Distribution Points:	URI
Certificate Policies:	OID
Subject alternative name:	Subscriber's E-mail address

For servers/services certificates:

Basic Constraints:	critical, ca: false
Subject Key Identifier:	Hash
Authority Key Identifier:	keyid
Key Usage:	critical,digitalSignature,keyEnciphermnet,dataEncipherment
Extended Key Usage	serverAuth,clientAuth
CRL Distribution Points:	URI

Certificate Policies:	OID
Subject alternative name:	DNS:FQDN

For CA certificate:

Basic Constraints:	Critical,ca:true
Subject Key Identifier:	hash
Authority Key Identifier:	keyid
Key Usage:	KeyCertSign, cRLSign
Subject alternative name:	ca-manager@ipm.ir

7.1.3 ALGORITHM OBJECT IDENTIFIERS

The OIDs for algorithms used for signatures of certificates issued by the IRAN-GRID CA are according to:

hash function:	id-sha	1 1.3.14.3.2.26
encryption:	rsaEncryption	1.2.840.113549.1.1.1
signature:	sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4 NAME FORMS

Each entity has a unique and unambiguous Distinguished Name (DN) in all the certificates issued to the same entity by the IRAN-GRID CA. The DN of the CA is "C=IR, O=IRAN-GRID,O=IPM, CN=IRAN-GRID CA". For the name forms of subscriber certificates the DN will be of the form defined in section 3.1.1.

7.1.5 NAME CONSTRAINTS

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

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

IRAN-GRID CA identifies this policy with the object identifier (O.I.D) 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)

The IRAN-GRID CA creates and publishes X.509 v2 CRLs.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

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

- The Authority Key Identifier
- The CRL Number

The CRL entry extensions that will be included are:

- CRL Reason Code
- Invalidity Date

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 IRAN-GRID CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.
The CA shall at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect. The auditor, as his/her discretion, may ask to carry out an audit at anytime, in particular, in the event of (or suspicion of) malpractice by CA or RA personnel, security flaws or complaints from subscribers or relying parties.
In addition, The IRAN-GRID CA will accept at least one external compliance audit per year when requested by a Relying Party. The entire cost of such an audit must be borne by the requestor.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Not defined

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The assessments are made by personnel of the IRAN-GRID CA or all eligible organizations of IRAN-GRID.
Member organizations of the EuGridPMA may undertake assessments if previously approved by EuGridPMA.
If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of IRAN-GRID CA's personnel and infrastructure.

8.4 TOPICS COVERED BY ASSESSMENT
The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY
In case of a deficiency, the IRAN-GRID CA Manager will announce the steps that will be taken to remedy the deficiency. This announcement will include a timetable.
If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

8.6 COMMUNICATION OF RESULTS
The CA Manager will make the result publicly available on the CA web site with as many details of any deficiency as she/he considers necessary.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES
No fees shall be charged

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES
See 9.1.

9.1.2 CERTIFICATE ACCESS FEE
See 9.1.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES
See 9.1.

9.1.4 FEES FOR OTHER SERVICES
No fees shall be charged.

9.1.5 REFUND POLICY

See 9.1.

9.2 FINANCIAL RESPONSIBILITY

No Financial responsibility is accepted for certificates issued under this policy.

9.2.1 INSURANCE COVERAGE
No stipulation.

9.2.2 OTHER ASSETS
No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES
No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION
No stipulation.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION
No stipulation.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION
No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

The IRAN-GRID CA service collects information about the subscribers. Information included in issued certificates and CRLs is not considered confidential.
The IRAN-GRID CA collects a subscriber's name, work telephone numbers and e-mail address. Additionally, for RA Managers and Operators, personal contact information is kept by the CA (work telephone number, work address).
Under no circumstances will the IRAN-GRID CA have access to the private keys of any subscriber to whom it issues a certificate.

9.4.1 PRIVACY PLAN
No stipulation.

9.4.2 INFORMATION TREATED AS PRIVATE
The information provided by the subscriber to verify his/her identity will be kept confidential.

9.4.3 INFORMATION NOT DEEMED PRIVATE

The IRAN-GRID CA collects the following information
From subscriber:

- Subscriber's full name
- Subscriber's organization
- Subscriber's organization unit
- Subscriber's public key

Which is not considered confidential.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

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

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

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

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

The CA will not disclose confidential information to any third party unless authorized to do so by the subscriber or when required by law enforcement officials who exhibit regular warrant.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Disclosure upon owner's request is done according to the Data Protection Law. Specifically, information is released to the subscriber if the CA has received a signed e-mail from the subscriber requesting the information. The CA charges no fee for this.

The CA will recognize requests in writing for the release of personal information from a subscriber provided the subscriber can be properly authenticated

9.5 INTELLECTUAL PROPERTY RIGHTS

The IRAN-GRID CA does not claim any intellectual property rights on certificates which it has issued.
This document is based on the following sources:

RFC 3647 [RFC3647] and RFC 2527 [RFC2527] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
RFC 1778 [RFC1778] The String Representation of Standard Attribute Syntaxes;

Parts in this document are inspired or even copied (in no particular order) from the: Magrid CA[MAgirdcpcps],TR-Grid CA [TRCPCPS],UFF BrGrid CA [BRCPCPS],UK e-Science CA [UKCPCPS]
PK-Grid CA[PK-GRID-CPCPS]
and indirectly from the documents on which they are based.
Anybody may freely copy from any version of the IRAN-GRID CA's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of the source.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

The IRAN-GRID CA guarantees to issue certificates only to subscribers identified by requests received from RAs via secure routes. The IRAN-GRID CA will revoke a certificate only in response to an authenticated request from the subscriber, or the RA which approved the subscriber's request, or if it has itself reasonable proof that circumstances for revocation are fulfilled.
The IRAN-GRID CA does not takes responsibility for problems arising from its operation or the use made of the certificates it provides and gives no guarantees about the security or suitability of the service.
The CA only guarantees to verify subscribers' identities according to procedures described in this document.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

All accredited RAs shall perform their task of identification of the requesting parties as described in 3.2.3 and 3.2.2 to the best of their knowledge. No other warranties are accepted.
An RA can conclude, at its strictly own risk, a more stringent agreement with its subscribers, but this shall never commit the IRAN-GRID CA nor any of its other accredited RAs. It is the RA's responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

By requesting a IRAN-GRID CA certificate a subscriber commits itself to use and protect the certificate and the certified keys according to the stipulations of the CP/CPS document in

effect at the date of issuance of the said certificate. She/he may however apply more stringent observances.
Subscribers must:
Read and adhere to the procedures published in this document

- Use the certificate for the permitted purposes only
- Authorize the processing and conservation of personal data (as required under the Data Protection Law)
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:

(Personal certificates) selecting a strong passphrase of at least 12 characters;
(Personal certificates) protecting the passphrase from others;

Notifying immediately the IRAN-GRID CA and any relying parties if the private key is lost or compromised;
Requesting revocation if the subscriber is no longer entitled to a certificate,
or if information in the certificate becomes wrong or inaccurate.

In case of a breach of stipulations of the CP/CPS document that the subscriber has agreed to by requesting the IRAN-GRID CA certificate the certificate shall be revoked immediately. No further warranties are required from the subscriber.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

A relying party must accept the subscriber's certificate for authentication purposes if:
The relying party must check the IRAN-GRID CA's CP and the CPS under which the certificate was issued before drawing any conclusion on trust of the subscriber's certificate; and

- The reliance is reasonable and in good faith in light of all circumstances known to the relying party at the time of reliance; and
- The certificate is used for permitted purposes only; and
- The relying party checked the validity and status of the certificate to their own satisfaction prior to reliance.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

The IRAN-GRID CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness.

Also the IRAN-GRID CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

9.8 LIMITATIONS OF LIABILITY

Except if explicitly dictated otherwise by the Iranian law the IRAN-GRID CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party. It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.
The CA does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted.

9.9 INDEMNITIES

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

9.10 TERM AND TERMINATION

9.10.1 TERM

This document becomes effective after its accreditation by EUGridMA and publication on the web site of the IRAN-GRID CA starting at the date announced there.
There is no term set for its expiration.

9.10.2 TERMINATION

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

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

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

9.12.2 NOTIFICATION MECHANISM AND PERIOD

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

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

Substantial changes shall cause the OID to be changed. The decision is made by the manager of the IRAN-GRID CA and submitted to the EUGridPMA for approval.

9.13 DISPUTE RESOLUTION PROVISIONS

Disputes arising out of the CP/CPS shall be resolved by the Manager of the IRAN-GRID CA.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

All activities relating to the request, issuance, use or acceptance of a IRAN-GRID CA certificate have to comply with the Iranian law.
Activities initiated from or destined for another country than Iran must also comply with that country's law

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

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

9.16.2 ASSIGNMENT
No provisions.

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

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)
No stipulation.

9.16.5 FORCE MAJEURE
In the case of Force Majeure the IRAN-GRID CA will make its best effort to maintain the service in accordance with its policy and will invoke the disaster recovery procedures as appropriate.

9.17 OTHER PROVISIONS
No stipulation.

10 REFERENCES

[RFC3647]	S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, " Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC 3647, November 2003 [replaces RFC 2527] http://www.ietf.org/rfc/rfc3647.txt
[RFC2527]	S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy andCertification Practices Framework" , RFC 2527, March 1999 http://www.ietf.org/rfc/rfc2527.txt
[RFC3280]	R. Housley, W. Polk, W. Ford and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" , RFC 3280, April 2002 http://www.ietf.org/rfc/rfc3280.txt
[RFC2119]	S. Bradner, " Key words for use in RFCs to Indicate Requirement Levels" RFC 2119, March 1997 http://www.ietf.org/rfc/rfc2119.txt
[RFC1778]	T. Howes, S. Kille, W. Yeong, C. Robbins , " The String Representation of Standard Attribute Syntaxes" RFC 1778, March 1995 http://www.ietf.org/rfc/rfc1778.txt

[RFC2252]	M. Wahl, A. Coulbeck, T. Howes, S. Kille, " Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions " RFC 2252, December 1997 http://www.ietf.org/rfc/rfc2252.txt
[ESCPCPS]	Certification Authority pkIRISGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.1, February 2006 http://www.irisgrid.es/pki/policy/1.3.6.1.4.1.7547.2.2.4.1.1.1/pkIRISGridCA_CP_ CPS_1_1_1.pdf
[SEECPCPS]	Certification Authority SeeGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.1, September 2004 http://www.grid.auth.gr/pki/seegrid-ca/documents/cps/SeeGridCA-CPS-1.1.pdf
[CRCPCPS]	Certification Authority SRCE CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.0, May 2006 http://ra.srce.hr/policy.pdf
[TRCPCPS]	Certification Authority TR-Grid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.0, June 2005 http://www.grid.org.tr/ca/policy/cpcps.pdf
[BRCPCPS]	Certification Authority UFF BrGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.0, July 2006 https://brgridca.ic.uff.br//index.php?option=com_docman&task=doc_download& gid=1&Itemid=13
[UKCPCPS]	UK e-Science Certification Authority Certificate Policy and Certification Practices Statement Version 1.3, 4 Aug 2006 http://www.grid-support.ac.uk/files/cps/cps-1.3.pdf
[MAGRIDCPCPS]	MaGrid CA ,Certificate Policy and Certification Practice Statement Version 1.2.0 https://ra.magrid.ma/ca/ra/policy/cp_cps_1_2_0.pdf
[PK-GRIDCPCPS]	PK-GRID-CA, Certificate Policy and Certification Practice Statement, http://www.ncp.edu.pk/pk-grid-ca/docs/cps-1.1.2.0.pdf

11 LIST OF CHANGES

18th March 2009 upgrading from RFC 2527 to RFC 3647