IRAN-GRID CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Document : 1.2.840.113612.5.4.2.7.1.1.1

Prepared By:

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

Table of Contents

1. Introduction

1.1 OVERVIEW

This document is based on the structure suggested by the RFC 2527. It defines the Certification Policy and the Certification Practice Statement of the IRAN-GRID CA Certification Authority and specifies the actual policies, practices, and obligations for the issuance and management of certificates. Terms used in this document are explained in the Glossary.

1.2 POLICY IDENTIFICATION

Document Title: **'IRAN-GRID CA Certificate Policy and Certification Practice Statement'**

Document O.I.D.: **1.2.840.113612.5.4.2.7.1.1.1**

IGTF	1.2.840.113612.5.4.2
IRAN-GRID CA Institute for studies in theoretical Physics and Mathematics (IPM)	.7
CP/CPS	.1
Major Version	.1
Minor Version	.1

Document Date: **April 2008.**

Expiration: This document is valid until further notice.

1.3 COMMUNITY AND APPLICABILITY

IRAN-GRID CA provides PKI services for scientific and academic communities of Iran, and IPM (Institute for studies in Theoretical Physics and Mathematics) partners working in grid related projects.

1.3.1 Certification Authorities

IRAN-GRID CA does not issue certificates to subordinate certification authorities.

1.3.2 Registration Authorities

The IRAN-GRID CA manages the functions of its Registration Authorities. Currently, IRAN-GRID CA performs the functions of Registration Authority.

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 End Entities

The IRAN-GRID CA will issue certificates to entities, which are based and/or having offices in Iran, and are intended for cross-organizational sharing of resources. All related activities must be open and public. The focus of these organizations should also be in research and/or education.

1.3.4 Applicability

There are three categories of certificates:

1. User certificates: authentication and communication encryption.
2. Host certificates: authentication and communication encryption.
3. Service certificates: authentication and communication encryption.

1.3.5 User Restrictions

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. The ownership of an IRAN-GRID CA does not imply complete authorization to access any kind of resources**.**

1.4 CONTACT DETAILS

The IRAN-GRID CA is created and managed by the Grid Computing Group (GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM).

The IRAN-GRID CA address for operational issues is:

IRAN-GRID Certification Authority
Grid Computing Group (GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM) ,Tehran - Iran, Phone: (+98 - 21) 22288680 Fax: (+ 98 -21) 22280415 Email: ca-manager@ipm.ir

The contact person for questions related with document is:

Majid Arabgol
Grid Computing Group (GCG), Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran, Phone: (+98 - 21) 22288680 Fax: (+ 98 -21) 22280415 Email: arabgol@ipm.ir

The contact person for IRAN-GRID CA related issues is:

Hessamaddin Arfaei
IPM deputy director, Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran, Phone: (+98 - 21) 22288680 Fax: (+ 98 -21) 22280415 Email:arfaei@ipm.ir

2. General Provisions

2.1 OBLIGATIONS

2.1.1 IRAN-GRID CA Obligations

The IRAN-GRID CA is responsible for the following aspects of issuance and management of certificates:

Issue and publish certificates based on validated requests.
Accept certification requests validated by the RA.
Deliver the certificate to end entity.
Accept revocation requests from RA's or end entities.
Ensuring that all aspects of the CA services, CA operations and CA infrastructure, related to certificates issued under this policy, are performed in accordance with the requirements, representations and warranties of this document.

2.1.2 IRAN-GRID RA Obligations

The IRAN-GRID RA is responsible for the following aspects, according to the procedures described in this document: (see 3.1.6)

- Authenticate entities requesting a certificate.
- Determine if the person requesting the certificate has the right to have an IRAN-GRID CA certificate.
- Send validated certificate requests to IRAN-GRID CA.
- Create and send validated revocation requests to the IRAN-GRID CA.
- Follow the policies and procedures described in this document.
- Inform IRAN-GRID CA when RA plans their organization.

The RA communicates with the IRAN-GRID CA via telephonic conversation which is followed by a signed e-mail by a valid IRAN-GRID CA certificate.

2.1.3 Subscriber Obligations

In all cases, the IRAN-GRID CA shall require the subscriber to:

Read and accept the policies and procedures published in this document.
Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key.
Use a strong passphrase with a minimum length of 12 characters to protect the private key of personal certificates.
Use the certificate exclusively for authorized and legal purposes, consistent with this policy.
Notify the IRAN-GRID CA when the certificate is no longer required.
Notify the IRAN-GRID CA when the information in the certificate becomes wrong or inaccurate.
Instruct the IRAN-GRID CA to revoke the certificate promptly upon an actual or suspected loss, disclosure, or other compromise of the subscriber's private key.
Accepts the statements relating to confidentiality of information in section 2.8.

2.1.4 Repository Obligations

The IRAN-GRID CA is responsible for providing a public repository, accessible through the World Wide Web at http://cagrid.ipm.ac.ir/
IRAN-GRID CA will publish:

- IRAN-GRID CA's Certificate (PEM, DER format).
- A periodically updated Certificate Revocation List (CRL) (PEM, DER format).
- A copy of a recent version of this policy and all previous versions.
- User and host certificates issued by the CA
- Contact addresses including physical address and email address.
- Other information that can be regarded as relevant to IRAN-GRID CA

The IRAN-GRID CA web site is maintained on a best effort basis. Excluding maintenance shutdowns and unforeseen failures, the site should be available 24 hours per day, 7 days a week.

2.1.5 Relying Party Obligations

A Qualified Relying Party is required to:

Accept the conditions and procedures described in this document.
Use the certificate exclusively for authorized and legal purposes, consistent with this Policy.
Verify the certificate revocation information before validating a certificate.

2.2 LIABILITY

2.2.1 IRAN-GRID CA Liability

IRAN-GRID CA guarantees only to authenticate the subjects requesting a certificate or revocation request according to the procedures described in this document; no other liability, neither implicit nor explicit is accepted.

IRAN-GRID CA is run on a best effort basis and does not give any guarantees about the service security or suitability.

IRAN-GRID CA will not be held liable for any problems arising from its operation or use made of certificates it issues.

IRAN-GRID CA denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

2.2.2 IRAN-GRID RA Liability

The Registration Authority:

Authenticates the identity of the subscribers requesting the certificates, according to the practices described in this policy.
Requests for revocation of a certificate if it is aware that the circumstances for revocation are satisfied.

2.3 FINANCIAL RESPONSIBILITY

IRAN-GRID CA will not accept any financial responsibilities.

2.4 INTERPRETATION

2.4.1 Governing Law

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

2.4.2 Dispute Resolution Procedures

Legal disputes arising from the operation of the IRAN-GRID CA will be resolved according to the law of Iran.

2.5 FEES

No fees are charged.

2.6 PUBLICATION AND REPOSITORIES

2.6.1 Publication of CA Information

The IRAN-GRID CA publishes the following information through its online repository at http://cagrid.ipm.ac.ir/:

- IRAN-GRID CA's Certificate (PEM, DER, format).
- User and host certificates that are issued in reference to this policy.
- A periodically updated Certificate Revocation List (CRL) (PEM, DER format).
- A copy of this policy, which specifies the CP and CPS.
- Contact addresses including physical address and email address.
- Other information relevant to the IRAN-GRID CA.

2.6.2 Frequency of Publication

Certificates will be published as soon as they are issued. CRLs will be published as soon as issued or at least after every 23 days. The life time of CRLs is 30 days. New versions of CP-CPS will be published as soon as they have been approved.

2.6.3 Access Controls

IRAN-GRID CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS.
The IRAN-GRID CA web site is maintained on best effort basis. Excluding maintenance shutdowns and unforeseen failures, the site should be available 24 hours per day, 7days a week.

2.7 COMPLIANCE AUDIT

IRAN-GRID CA declares that their practices fully comply with this CP-CPS. Requests for external audit from other trusted CA will be accepted at the discretion of Institute for studies in theoretical Physics and Mathematics (IPM) with the consideration that all costs associated with such an audit will be borne by the requesting party.

2.7.1 Frequency of Entity Compliance Audit

No Stipulation.

2.7.2 Identity/qualifications of auditor

No Stipulation.

2.7.3 Auditor's relationship to audited party

No Stipulation.

2.7.4 Topics covered by audit

No Stipulation.

2.7.5 Actions taken as a result of deficiency

No Stipulation.

2.7.6 Communication of results

No Stipulation.

2.8 CONFIDENTIALITY POLICY

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

Subscriber's full name.
Subscriber's e-mail address.
Subscriber's organization.
Subscriber’s organizational unit.
Subscriber's public key.

2.8.1 Confidential Information kept by the IRAN-GRID CA

Record of the e-mail messages sent and received by the IRAN-GRID CA is considered confidential. Under no circumstances the IRAN-GRID CA does have access to the private keys of the subscribers to whom it issues a certificate.

2.8.2 Types of Information not considered Confidential

Data contained in the CRLs and the subscriber certificate shall not be considered confidential and will be published in a publicly accessible location.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

The IRAN-GRID CA will notify and inform the following entities:

The subject of the personal certificate.
The requester of the server certificate.

2.8.4 Release of Information to Law Enforcement Officials

The IRAN-GRID CA will not disclose any information to any third party, aside from information publicly available, except when so required by a legal authority of competent jurisdiction.

2.8.5 Information that can be revealed as a Part of Civil Discovery

See section 2.8.4

2.8.6 Conditions of Disclosure upon owner's request

See section 2.8.1

2.8.7 Other Circumstances for Disclosure of Confidential Information

See section 2.8.4

2.9 INTELLECTUAL PROPERTY RIGHTS

Parts of this document are inspired by cp/cps of [CERN CA], [ASGCCA CA] , [PK-GRID CA], [MaGrid CA] and [BEgrid CA].

3. Identification and Authentication

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The subject distinguished names (DNs) for the certificate applicants shall follow the X.501 standard:

- In case of personal certificate the subject name must include the person's full name
- In case of server certificate the subject name must include the DNS FQDN.

3.1.2 Name Meanings

Each entity has a clear and unique Distinguished Name (DN) in the certificate subject field.
Any name under this CP-CPS will have "C=IR, O=IPM".

For a user certificate the common name (CN) must be the full name of the subscriber.
In case the subscriber belongs to the host the CN must be the FQDN of the server:

Illustration of a full subject distinguished name for a user:
C=IR, O=IPM, 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=IPM, 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=IPM,O=Sharif University of Technology , OU= Physics Dept, CN=ldap/grid02.sharif.ac.ir

3.1.3 Name Uniqueness

The name listed in a certificate shall be unambiguous and unique for all certificates issued by the IRAN-GRID CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the name to ensure uniqueness. Certificates must apply to unique individuals or resources. Users must not share certificates.

3.1.4 Verification of Key Pair

No Stipulation.

3.1.5 Authentication of Organization

IRAN-GRID CA verifies the Authentication of Organization by checking that:

The organization is known to be part of an international grid-computing project or part of an international and scientific Virtual Organization (VO).

The organization operates in Iran and is part of an academic or research institute recognized by the Iranian Ministry of Science , Research and Technology and/or the Iranian Minstry of Health and medical education.

The information of authenticated organization is published on http://cagrid.ipm.ac.ir/auth.htm

3.1.6 Authentication of Individual

3.1.6.1 Person requesting a certificate

The subscriber must contact personally the CA/RA staff in order to verify his identity and the validity of the request.
The subscriber authentication is performed through the presentation of a valid official identification document: passport; national identity card.

3.1.6.2 Host certificate

Host certificates can only be requested by the administrator responsible for the particular host. In order to request a host certificate, the administrator must already possess a valid personal IRAN-GRID certificate.

3.2 ROUTINE REKEY

Rekey of certificates will follow the same authentication procedure as new certificate. A request for rekeying of a certificate must be submitted prior to certificate expiration.

3.3 REKEY AFTER REVOCATION

Revoked or expired certificates shall not be renewed. Applicants without a valid certificate from the IRAN-GRID CA shall be re-authenticated by the RA on certificate application, just as with a first time application.

3.4 REVOCATION REQUESTS

Certificate revocation requests should be submitted by:

E-mail sent to ca-manager@ipm.ir signed with a valid IRAN-GRID CA certificate
When e-mail is not an option, the request will be authenticated using the procedure described in section 3.1.6.

4. Operational Requirements

4.1 CERTIFICATE APPLICATIONS

The necessary provisions that must be followed in any certificate application request to the IRAN-GRID CA are:

- The applicant must be an acceptable end user entity, as defined by this policy.
- The applicant must contact the local RA and provide necessary documents for the RA manager.
- The applicant will be notified by RA manager via e-mail whether the request is approved or rejected.
- In the case of rejection she/he will be given reasons and In the case of approval the applicant must generate her/his own key pair by requesting a CSR(Certificate Signing Request). Application should be made via ssl protected on-line webpage https://cagrid.ipm.ac.ir.

- The applicant must obey the IRAN-GRID CA distinguished name scheme and the distinguished name must be unambiguous and unique.
- The IRAN-GRID CA by no way must know or generate private key for an applicant.

The default validation period is one (1) year.

4.2 CERTIFICATE ISSSUANCE

Following are the requirements for a certificate to be issued:

The subscriber authentication must be successful.
The key must have 1024 bits.
The maximum validity period for a certificate must be 1 year.

The subscriber will be notified by e-mail about the certificate issuance or rejection. In the case of rejection the e-mail will state the reason.

4.3 CERTIFICATE ACCEPTANCE

Not defined.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances of Revocation

A certificate will be revoked in the following circumstances:

The subject of the certificate has ceased his relation with the grid projects.
The subject does not require the certificate any more.
The private key has been lost or is suspected to be compromised.
The information in the certificate is wrong or inaccurate.
The system to which the certificate has been issued has been retired.
The subject has failed to comply with the rules of this policy.

4.4.2 Who can Request Revocation

The revocation of the certificate can be requested by:

The certificate subscriber.
Any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data.
The Registration Authorities (RAs).
The IRAN-GRID CA.

4.4.3 Procedure of Revocation Request

The entity requesting the revocation must send the revocation request by signed e-mail to the IRAN-GRID CA/RA. If this is not possible the CA/RA must be contacted directly. Authentication can be performed as described in 3.1.6.

4.4.3.1 Repository/CRL Update

The CRL or certificate status database in the repository, as applicable, shall be updated immediately after revocation. All revocation requests and the resulting actions taken by the IRAN-GRID CA shall be archived.

4.4.4 Certificate Suspension

There is no provision for certificate suspension.

4.4.5 Who can request suspension?

No Stipulation.

4.4.6 Procedure for suspension request

No Stipulation.

4.4.7 Limits on Suspension Period

No Stipulation.

4.4.8 CRL Issuance Frequency

CRLs are issued after every certificate revocation or at least every 23 days.

4.4.9 CRL Checking Requirements for Relying Parties

Before using any certificate the relying parties should check the CRL. No access control shall limit the possibility to check the CRL.

4.4.10 On-line Revocation/Status Checking Availability

Not defined.

4.4.11 On-line Revocation Checking Requirements

Not defined.

4.4.12 Other Forms of Revocation Advertisement

Not defined.

4.4.13 Variations of the above in case of private key compromise

Not defined.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 Types of Events Audited

Boots and shutdowns of the equipment
Interactive system logins

4.5.2 Processing Frequency of Audit Logs

Audit logs will be analyzed at least once per month.

4.5.3 Retention Period of Audit Logs

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

4.5.4 Protection of Logs

Only authorized IRAN-GRID CA personnel is allowed to view and process audit logs. Audit logs are copied to an offline medium.

4.5.5 Backup Procedures

Audit logs are copied to an offline medium, which is safely stored.

4.5.6 Accumulation system

The audit log accumulation system is internal to the IRAN-GRID CA.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Records Archived

The following data and files will be archived by the IRAN-GRID CA:

All certificate requests (including certification and revocation).
All issued certificates and all issued CRLs.
All the e-mail messages sent and received by the IRAN-GRID CA.

4.6.2 Retention Period for Archives

Logs will be kept for a minimum of three (3) years.

4.6.3 Protection of Archive

Records are backed up on removable media, which are safely stored.

4.6.4 Archive Backup Procedures

Records are archived as soon as a certificate/CRL is issued or at least after every 23 days.

4.6.5 Archive Collection System

The archive collection system is internal to the IRAN-GRID CA.

4.7 KEY CHANGEOVER

In 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 certificates, the older but still valid certificate must be available to verify old signatures – and the private key to sign CRLs – until all 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.

As the key generation is carried out by each end entity (subscriber) by, for example, using a web browser, no provision is made by the IRAN-GRID CA for a key changeover for the CA's user.

4.8 COMPROMISE AND DISASTER RECOVERY

If the IRAN-GRID CA private key is destroyed, compromised or suspected to be so the IRAN-GRID CA will:

- Notify subscribers and other relying parties.
- Terminate the issuance and distribution of certificates and CRLs.
- Notify relevant security contacts.
- Notify all cross-certifying CAs

4.9 CA TERMINATION

Upon termination the IRAN-GRID CA will:

Notify subscribers and Relying Parties.
Terminate the issuance and distribution of certificates and CRLs.
Notify relevant security contacts.
Notify as widely as possible the end of the service.
Notify all cross-certifying CAs

5. Physical, Procedural and Personnel Security Controls

5.1 PHYSICAL SECURITY – ACCESS CONTROLS

5.1.1 Site Location

The IRAN-GRID CA is located at Institute for studies in theoretical Physics and Mathematics (IPM), Niavaran Square, Niavaran Bldg., Tehran, Iran.

5.1.2 Physical Access

Physical access to the IRAN-GRID CA's repository and CA/RA computers are restricted to authorized personnel.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the repository machines are connected to a UPS system.

5.1.4 Water Exposures

No Stipulation.

5.1.5 Fire Prevention and Protection

The on-line computers are in a room equipped by fire protection systems. And the off-line computer is in fire-safe

box in the same room.

5.1.6 Media Storage

The IRAN-GRID CA key and Back-up copies of IRAN-GRID CA related information is kept in several removable storage media.

5.1.7 Waste Disposal

Waste carrying potential confidential information, such as old floppy disks, are physically destroyed before being trashed.

5.1.8 Off-site Backup

No off-site backups are currently performed.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Not defined.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background Checks and Clearance Procedures for CA Personnel

IRAN-GRID CA personnel are recruited from Institute for Studies in Theoretical Physics and Mathematics (IPM).

5.3.2 Background Checks and Security Procedures for other personnel

No other personnel are authorized to access the IRAN-GRID CA facilities without the physical presence of IRAN-GRID CA personnel.

5.3.3 Training Requirements and Procedures

Not defined.

5.3.4 Training Period and Retraining Procedures

Not defined.

5.3.5 Frequency and Sequence of Job Rotation

No job rotation is performed.

6 TECHNICAL SECURITY CONTROL

6.1 Key pair generation and installation

6.1.1 Key pair generation

Each subscriber must generate his/her own key pair. The IRAN-GRID CA does not generate private keys for subjects.

6.1.2 Private Key delivery to Entity

The IRAN-GRID CA does not generate private keys hence does not deliver private keys.

6.1.3 Subscriber Public Key Delivery to IRAN-GRID CA

The applicant must deliver her/his public key by submitting a Certificate Signing Request (CSR) according the procedure explained in section 4.1.

6.1.4 CA Public Key delivery to users

After signing of the successful applicant's CSR she/he will be notified by an email from IRAN-GRID CA admin(ca-manager@ipm.ir).
IRAN-GRID CA certificates can be downloaded from the IRAN-GRID CA web site at: http://cagrid.ipm.ac.ir

6.1.5 Key Sizes

- The key length for a personal or server certificate is 1024 bits.
- The IRAN-GRID CA key length is 2048 bits

The algorithm used for key generation by the IRAN-GRID CA is RSA.

6.1.6 Public Key Parameters Generation

Not defined.

6.1.7 Parameter quality testing

Not defined.

6.1.8 Hardware/software key generation

Not defined.

6.1.9 Key Usage Purposes

The CA private key is used to sign certificates and CRLs(keyCertSign, crlSign).

Private Key for end entity is used for digital signature, proxy creation (digitalSignature , keyEncipherment) and data encryption, message integrity (dataEncipherment).

6.2 PRIVATE KEY PROTECTION

6.2.1 Private Key (n out of m) Multi-Person Control

Not defined.

6.2.2 Private Key Escrow

IRAN-GRID CA keys are not given in escrow.

6.2.3 Private Key Archival and Backup

The IRAN-GRID CA private key is kept encrypted in multiple copies in several removable storage media in safe places. The passphrase is in a sealed envelope kept in a safe place.

6.2.4 Private Key backup

The private keys of the IRAN-GRID Certification Authority are backed up on a removable media, stored in a secure place.

6.2.5 Private Key archival

Backup copies made are never destroyed and may be used as an archival service.

6.2.6 Private Key entry into cryptographic module

The private key of the IRAN-GRID Certification Authority is stored in encrypted form only, and protected by a pass phrase of at least 15 characters.

6.2.7 Method of activating private key

The activation of the CA private key is by providing the pass phrase.

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

No stipulation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

The IRAN-GRID CA private key is valid for 5 years.

6.4 ACTIVATION DATA

The IRAN-GRID CA private key is protected by a passphrase with a minimum length of 15 characters.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Security Technical Requirements

The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches.

CA systems configuration is reduced to the bare minimum.

The signing machine is kept powered off between uses.

6.5.2 Computer Security Rating

Not defined.

6.6 LIFE CYCLE SECURITY CONTROLS

Not defined.

6.7 NETWORK SECURITY CONTROLS

The CA signing machine is kept off-line.

The RA-public machines other than the signing machine are protected by a firewall.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Not defined.

7. Certificate and CRL profile

7.1 CERTIFICATE PROFILE

7.1.1 Version

All certificates that refer to this policy will be issued in the X.509 version 3 format and will include a reference to the O.I.D. of this Policy within the appropriate field.

7.1.2 Certificate Extensions

For natural person certificates:

a. Basic Constraints: critical, ca: false
b. Subject Key Identifier: hash
c. Authority Key Identifier: keyid,issuer:always
d. Key Usage: critical, digitalSignature, keyEncipherment,
e. Extended Key Usage :clientAuth, emailProtection
f. CRL Distribution Points: URI
g. Subject alternative name: Subscriber's E-mail address
h. Certificate policies :OID

For servers/services certificates:

a. Basic Constraints: critical, ca: false
b. Subject Key Identifier: hash
c. Authority Key Identifier: keyid,issuer:always
d. Key Usage: critical, digitalSignature, keyEncipherment,dataEncipherment
e. Extended Key Usage :serverAuth, clientAuth
f. CRL Distribution Points: URI
g. Subject alternative name: Server's DNS FQDN host name
h. certificate policies :OID

For CA certificate:

a. Basic Constraints: critical, ca: true
b. Subject Key Identifier: hash
c. Authority Key Identifier keyid,issuer:always
d. Key Usage: critical, KeyCertSign, cRLSign

7.1.3 Algorithm Object Identifiers

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

- 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

- Issuer: C=IR, O=IPM, CN=IRAN-GRID CA
- Subject (Persons): C=IR, O=IPM, O=<AUTH.ORG>,OU=<ORG UNIT>, CN=<FULL NAME>

- Subject (Hosts):C=IR,O=IPM,O=<AUTH.ORG> OU=<ORG.UNIT>, CN=<FQDN>
- Subject (services):C=IR,O=IPM, O=<AUTH.ORG>,OU=<ORG UNIT>, CN=<service/FQDN>

7.1.5 Name Constraints

See section 3.1.2

7.1.6 Certificate Policy Identifier

See section 1.2

7.1.7 Policy Qualifier Syntax and Semantics

Not defined.

7.2 CRL PROFILE

7.2.1 Version number(s)

All CRLs will be CRL version 2 format

7.2.2 CRL and CRL entry Extensions

No stipulation.

8 SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Users will not be warned in advance of changes to IRAN-GRID CA's policy and CPS. Revision is made and approved by the EUgridPMA. Minor editorial changes to this document can be made without approval by the EUgridPMA. New OID will
not be assigned to the revised document when minor changes would be made. Major changes
such as changes in policy or technical security controls need to be approved by the European GRID PMA. New OID will be assigned to the
revised document for such major changes made.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The IRAN-GRID CA policy is available at http://cagrid.ipm.ac.ir/policy.htm

8.3 CPS APPROVAL PROCEDURES

No Stipulation.

Glossary

Activation Data

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

Certification Authority (CA)

The entity / system that 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).

Certificates – or Public Key Certificates

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

Certificate Policy (CP)

A named set of rules indicates the applicability of a certificate to a particular community and/or class of application 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 for the trading of goods within a given price range.

Certification Practice Statement (CPS)

A statement of the practices, a CA employs in issuing certificates.

Certificate Revocation Lists (CRL)

A CRL is a time stamped list identifying revoked certificates that is signed by a CA and made freely available in a public repository.

End Entity

A certificate subject that does not sign certificates (i.e., personal and host certificates).

Host Certificate

A certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine.

IPM

Institute for studies in Theoretical Physics and mathematics

Public Key Infrastructure (PKI)

A term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. All of this implies a set of standards for applications that use encryption.

Personal Certificate

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

Policy Qualifier

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

Private Key

In a PKI, a cryptographic key created and kept private by a subscriber. It may be used to make digital signatures which may be verified by the corresponding public key; to decrypt the message encrypted by the corresponding public key; or, with other information, to compute a piece of common shared secret information.

Public Key

In a PKI, a cryptographic key created and made public by a subscriber. It may be used to encrypt information that may be decrypted by the corresponding private key; or to verify the digital signature made by the corresponding private key.

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).

Relying Party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

RSA

RSA is named after its creators Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman. It is the most popular public key algorithm currently in use. It is so popular because it provides secrecy, authentication and encryption all in one little package.

Subscriber

In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.

SSL

Secure Socket Layer is a protocol that transmits our communications over the network in an encrypted form and ensures that the information is sent unchanged, only to the computer we intended to send it to.