TR-GRID

CERTIFICATION AUTHORITY

CERTIFICATE POLICY

AND

CERTIFICATION PRACTICE STATEMENT

Version 2.2

September, 2009

Table of Contents:

1. INTRODUCTION

1.1 Overview

This document is organized according to the specifications proposed by the RFC 3647. It describes the procedure followed by TR-GRID (National Grid Initiative of Turkey) Certification Authority and is the combination of Certificate Policy and Certification Practice Statement (CP/CPS).

This document is a valid CP/CPS as of October 15, 2009, 09:00 UTC.

1.2 Document Name and Identification

Document Title

TR-GRID CA Certificate Policy and Certification Practice Statement

Document Version

2.2

Document Date

October 15, 2009

ASN.1 Object Identifier (OID)

1.3.6.1.4.1.23658.10.1.2.2

1.3 PKI Participants

1.3.1 Certification Authorities

The TR-GRID CA does not issue certificates to subordinate Certification Authorities.

1.3.2 Registration Authorities

The TR-GRID CA assigns the authentication of individual identity to Registration Authorities (RA). Based on this CP/CPS document, RAs are not allowed to issue certificates. The list of RAs is available on the TR-GRID CA website.

1.3.3 Subscribers

TR-GRID CA provides PKI services to meet the requirements of Turkish academics and research communities including national or international Grid activities.

TR-GRID CA issues certificates to the following entities:

- Users (people)
- Computers (hosts)
- Services (host applications)

1.3.4. Relying Parties

All entities that use public keys of certificates, issued by TR-GRID CA, for signature verification and/or encryption, will be considered as relying parties.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

User certificates can be used to authenticate a user that would like to benefit from the academic resources, services and activities including Grid resources.

Host certificates can be used to identify computers that have special tasks related to the Grid or other academic activities.

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

In addition, user certificates can be used for e-mail signing and encryption (S/MIME).

User certificates must not be shared.

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

TR-GRID Security Group at TUBITAK ULAKBIM is in charge of the management of TR-GRID CA.

Phone: +90 312 2989365
E-mail: ca@grid.org.tr

Address: YOK Binasi B5 Blok 06539
Bilkent, Ankara
Turkey

1.5.2 Contact Person

The contact person that can deal with any questions related to this document or operational issues:

Feyza Eryol

Phone: +90 312 2989304
E-mail: feyza@ulakbim.gov.tr

Address: YOK Binasi B5 Blok 06539
Bilkent, Ankara
Turkey

Website: http://www.grid.org.tr/ca

1.5.3 Person Determining CPS Suitability for the Policy

The person mentioned in 1.5.2.

1.5.4 CPS Approval Procedures

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

1.6 Definitions and Acronyms

Activation Data: Data values, different from keys, that are required to operate cryptographic modules and that need to be protected such as a pin or a passphrase.

CA – Certification Authority: The entity / system that signs X.509 identity certificates**.**

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

CPS – Certification Practice Statement: A statement for the practices, that a certification authority applies in its operations.

CRL – Certificate Revocation List: A time stamped list displaying revoked certificates that are signed by a CA and made freely available in a public repository.

PKI – Public Key Infrastructure: IT infrastructure that enables users of a basically unsecure public network (such as the Internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Private Key: In secure communication, an algorithmic pattern used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key.

Public Key: The pattern used to confirm "signatures" on incoming messages or to encrypt a file or message so that only the holder of the private key can decrypt the file or message.

RA – Registration Authority: An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Relying Party: A recipient who accepts a digital certificate and digital signature.

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.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

TR-GRID CA will maintain a secure on-line repository at http://www.grid.org.tr/ca that includes:

- The TR-GRID CA root certificate
- A http URL of the PEM-formatted CA certificate
- A periodically updated http URL of the PEM formatted CRL
- A periodically updated http URL of the DER formatted CRL
- User and host certificates issued by the CA
- All versions (current and past) of its verified CP/CPS document
- An official contact e-mail address
- A physical contact address
- Other information that can be regarded as relevant to TR-GRID CA

The on-line repository runs on best-effort basis with an availability of 24x7, liable to reasonable scheduled maintenance.

2.2 Publication of Certification Information

See section 2.1.

2.3 Time or Frequency of Publication

- Certificates will be put to the TR-GRID CA website as soon as they are issued.
- CRL publication will be updated immediately after a revocation is issued and it will be updated at least 7 days before the expiration date of the CRL where CRL life time is 30 days.
- New versions of all TR-GRID CA documents will be published on the website as soon as they are updated.
- New versions of this CP/CPS document will be published soon after they are validated and former versions will be kept as a record in the repository.

2.4 Access Control on Repositories

The on-line repository is available on a 24x7 basis, liable to reasonable scheduled maintenance.

TR-GRID CA does not impose any access control on the policy, issued certificates, and the CRLs.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The subject name in the end-entity certificates is in X.509v3 format and compliant with RFC3280. Any name under this CP/CPS is in the form of "C=TR, O=TRGrid, OU=unit". The following part is the "CN" which is distinguished for each person or each host.

- Illustration of a full subject distinguished name for a user:
  C=TR, O=TRGrid, OU=Ulakbim, CN=Asli Zengin
- Illustration of a full subject distinguished name for a host:
  C=TR, O=TRGrid, OU=Ulakbim, CN=host1.ulakbim.gov.tr
- Illustration of a full subject distinguished name for a service:
  C=TR, O=TRGrid, OU=TRGrid, CN=ldap/ldap.grid.org.tr

3.1.2 Need for Names to be Meaningful.

The Subject Name in a certificate must have a logical relation with the identity name of the subscriber, preferably, it can be the actual name of the user. If it is a host certificate, the CN must be stated as the fully qualified domain name (FQDN). Each host certificate must be linked to a single network entity.

3.1.3 Anonymity or Pseudonimity of Subscribers

TR-GRID CA does not issue pseudonymous or anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

See section 3.1.1.

3.1.5 Uniqueness of Names

The subject name included in the CN part of a certificate must be unique for all certificates issued by the TR-GRID CA. When essential, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of a Key

Requests are submitted via SSL protected HTTP transport, either in PKCS10 or SPKAC format. Host or service certificates can be submitted by signed e-mail. In all cases, signature is verified by the CA.

3.2.2 Authentication of Organization Identity

Not yet assigned.

3.2.3 Authentication of Individual Entity

Certificate of a person:

- The subject should contact personally the RA staff in order to validate his/her identity.
- The subject authentication is fulfilled by providing an official document (ID-card, driving license or a passport) declaring that the subject is a valid end entity.

In exceptional cases such as remote geographical location of the subject, identity validation may be performed by video conference. In this case, an authenticated photocopy of the required document (ID-card, driving license or a passport) must be delivered by mail or courier to the RA staff prior to this online meeting. Authenticated photocopy refers to the verification made by a legally accepted notary public under Turkish law.

Certificate of a host:

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 TR-GRID certificate.

3.2.4 Non-verified Subscriber Information

During the initial identity validation the requester's e-mail is not verified.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria of Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Expiration warnings will be sent to subscribers before it is re-key time. Re-key before expiration can be executed by stating a re-key request signed with the personal certificate of the subscriber but after 3 years face-to-face identity validation is required as described in 3.2.3. Re-key after expiration uses completely the same authentication procedure as new certificate.

3.3.2 Identification and Authentication for Re-key after Revocation

A revoked certificate shall not be renewed. The procedure for re-authentication is exactly the same with an initial registration.

3.4 Identification and Authentication for Revocation Request

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

- By signing a revocation request e-mail via a valid personal TR-GRID certificate
- By personal authentication as described in 3.2.3.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

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

- The subject must be appropriate to the specifications stated in this policy.
- The key length of a certificate must be 1024 or 2048 bits.
- Each applicant generates his/her own key by using OpenSSL or similar software.
- Maximum life time of a certificate is 1 year.
- Message digests of the certificates must be generated by SHA1 algorithm.
- Host and service certificate requests must be submitted via SSL protected HTTP transport or via e-mail signed by a valid TR-GRID CA certificate to the appropriate RA.
- For host and service certificates, the requester must be appropriately authorized by the owner of the FQDN.
- User certificate requests must be submitted via SSL protected HTTP transport.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

For a certificate to be issued, the subject authentication must be successful and proper as specified in this document. Applicants will be informed about the status of their certificate whether it is issued or rejected.

4.2.2 Approval or Rejection of Certificate Applications

If the certificate request does not meet one or more of the criteria in 4.1.1, it will be rejected and the requester will be informed via e-mail.

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

CA will check that identity validation is properly performed as described in 3.2.3.
CA will ensure secure communication with RAs by signed e-mails, SSL protected private web pages and voice conversations with a known person.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Applicants will be notified via e-mail when the certificate is issued and the issued certificate will be hosted at the online CA repository.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers of TR-GRID CA are required to agree with the following issues:

- acknowledgment of conditions and loyalty to the procedures interpreted in this document
- permanent provision of correct information to the TR-GRID CA and avoidance of unnecessary information out of purposes of this document
- use of the certificate for only authorized purposes that are stated in this document
- admission of restrictions to liability defined in section 9.8
- admission of statements about confidentiality of information emphasized in section 9.4
- key pair (public key and private key) generation using a secure method
- acceptable precautions against loss, disclosure or illegal use of the private key
- notifying TR-GRID CA in case private key is compromised or lost
- notifying TR-GRID CA in case of information change in the certificate
- notifying TR-GRID CA in case the subscriber requests to revoke the certificate

4.4.2 Publication of the Certificate by the CA

All the certificates issued by TR-GRID CA will be published at the on-line CA repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

See section 4.3.2.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

See section 1.4.1.

4.5.2 Relying Party Public Key and Certificate Usage

So as to use TR-GRID CA certificates, relying parties must consider the following specifications:

- loyalty to all the statements in this document
- use of the certificate for only authorized purposes
- checking CRL list from the website before validating a certificate

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Certificate renewal is not permitted. Subscribers must follow the re-key procedure, described in 3.3.1.

4.6.2 Who may Request Renewal

See section 4.6.1.

4.6.3 Processing Certificate Renewal Requests

See section 4.6.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

See section 4.6.1.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See section 4.6.1.

4.6.6 Publication of the Renewal Certificate by the CA

See section 4.6.1.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.6.1.

4.7 Certificate Re-key

4.7.1 Circumstances for Certificate Re-key

The following circumstances require certificate re-key:

- expiration of subscriber's certificate,
- revocation of subscriber's certificate.

4.7.2 Who may Request Certification of a New Public Key

Any subscriber holding a valid TR-GRID CA end entity certificate can request certificate re-key.

4.7.3 Processing Certificate Re-keying Requests

See sections 3.3.1 and 3.3.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

No stipulation.

4.8.2 Who may Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate will be revoked in the following situations:

- The subscriber does not need the certificate any more.
- The subscriber has not obeyed the stated obligations.
- The information in the certificate is incorrect.
- The private key of a certificate is lost, compromised or suspected to be compromised.

In one of the conditions above, end entity must request revocation of the certificate as soon as possible but within one working day.

4.9.2 Who can Request Revocation

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

4.9.3 Procedure for Revocation Request

Revocation requests should be submitted in one of the following ways:

- by email sent to ca@grid.org.tr
- personally at the RA/CA

All revocation requests should be properly authenticated as described in 3.4.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time within which CA must Process the Revocation Request

TR-GRID CA will process all revocation requests within 1 working day.

4.9.6 Revocation Checking Requirement for Relying Parties
A relying party must verify the certificate that it uses considering the most recently issued CRL.

4.9.7 CRL Issuance Frequency
See section 2.3.

4.9.8 Maximum Latency for CRLs
No stipulation.

4.9.9 On-line Revocation/status Checking Availability
At present, no on line service for this purpose is available.

4.9.10 On-line Revocation Checking Requirements
See section 4.9.9.

4.9.11 Other Forms of Revocation Advertisements Available
No stipulation.

4.9.12 Special Requirements Re-key Compromise
No stipulation.

4.9.13 Circumstances for Suspension
TR-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
TR-GRID CA online repository contains list of valid certificates and list of revoked certificates (CRL). Both lists are continuously updated.

4.10.2 Service Availability
The on-line repository is available on a 24x7 basis, liable to reasonable scheduled maintenance.

4.10.3 Optional Features
No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The TR-GRID CA operates in a controlled and protected room in TUBITAK ULAKBIM building.

5.1.2 Physical Access

Physical access to the hardware (entering the computer room) is restricted to the authorized personnel.

5.1.3 Power and Air Conditioning

No stipulation.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

TUBITAK ULAKBIM building has a fire alarm system.

5.1.6 Media Storage

Backups are to be stored in removable storage media.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

No stipulation.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Access to servers and applications is limited to the TR-GRID CA Security Personnel who are staff in TUBITAK ULAKBIM.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Internal training is available and applied to the TR-GRID CA and RA operators.

5.3.4 Retraining Frequency and Requirements

TR-GRID CA will perform operational audit of the CA and RA operators once a year. Retraining is applied if the audit results are not satisfactory.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

Operational manual for CA and RA operators is supplied to the new TR-GRID CA personnel.

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

The login/logout/reboot information of the issuing machine is archived. In addition, annual operational audits of CA/RA staff must be performed.

5.4.2 Frequency of Processing Log

No stipulation.

5.4.3 Retention Period for Audit Log

Minimum retention period is three years.

5.4.4 Protection of Audit Log

Archives are kept in a separate room with limited access.

5.4.5 Audit Log Backup Procedures

Audit logs are kept in removable storage media in a safe room with restricted access.

5.4.6 Audit Collection System (Internal vs. External)

Audit log collection system is internal to TR-GRID CA.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

No stipulation.

5.5 Records Archival

5.5.1 Types of Records Archived

The TR-GRID RA will archive the following items:

- Application data (certificate and revocation requests)
- Issued certificates and CRLs
- All e-mail messages correspondence with TR-GRID CA and RA
- The login/logout/reboot information of the issuing machine

5.5.2 Retention Period for Archive

Minimum retention period is three years.

5.5.3 Protection of Archive

Archives are kept in an auditable form with limited access.

5.5.4 Archive Backup Procedures

All archive data are copied to removable storage media.

5.5.5 Requirements for Time-stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation

5.6 Key Changeover

Lifetime of TR-GRID CA is 20 years and lifetime of end entity certificates is 1 year. The CA's private key is changed periodically; from that time on, the new key will be valid in order to sign new certificates or CRL lists of new certificates. The overlap of the old and new key must be at least one year. The older but still valid certificate must be available to verify old signatures and its private key must be used to sign CRLs until all the certificates signed using the associated key have expired or been revoked.

5.7 Compromise and Disaster Recovery

If the CA private key is compromised or destroyed in some way, the CA will perform the following tasks:

- Inform the EuGridPMA
- Inform all the nodes, RAs and other relying parties
- Conclude the issuance and distribution of certificates and CRLs
- Generate a new CA certificate with a new key pair that will be soon available on the website.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

No stipulation.

5.7.3 Entity Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

5.8 CA or RA Termination

TR-GRID CA will do the following tasks before it terminates its Grid-related services:

- Inform the subscribed users and RAs

- Stop to issue certificates and CRLs
- Notify the relevant security contacts
- Declare its termination on the website
- Annihilate all copies of private keys

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

Applicants can make host/service certificate requests to the RA via e-mail signed by a valid TR-GRID CA certificate. Applicant's public keys are delivered to the RA in an email containing the certificate request. The public key arrives at the TR-GRID CA in an email signed by the RA.

Applicants can make user/host/service certificate requests via SSL protected HTTP certification request service provided by the RA.

6.1.4 CA Public Key Delivery to Relying Parties

The TR-GRID CA root certificate is available on the website: http://www.grid.org.tr/ca

6.1.5 Key Sizes

For a user or host certificate the key size is 1024 or 2048 bits. The TR-GRID CA key size is 2048 bits.

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

TR-GRID certificates may be used only for authentication and signing proxy certificates, e-mail signing and encryption.
TR-GRID CA private key will only be used to issue CRLs and new certificates and to revoke certificates.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The TR-GRID CA uses sha1 with RSA encryption as a signature algorithm.

6.2.2 Private Key (n out of m) Multi-person Control

No stipulation.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

TR-GRID CA does not archive private keys apart from the private key corresponding to the root certificate of TR-GRID CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module

TR-GRID CA does not use cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

See section 6.2.6.

6.2.8 Method of Activating Private Key

TR-GRID CA private key is protected by a passphrase of at least 15 characters and only known by authorized CA personnel.
The subscriber is required to generate a secure pass phrase, at least 12 characters long for the private key. Private key cannot be shared and it is subscriber's responsibility to protect the private key properly.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

No stipulation.

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

TR-GRID CA root certificate has a validity of twenty years. For subscribers, the maximum validity period for a certificate is one year.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

TR-GRID CA does not generate activation data for subscribers. The subscriber is required to generate a secure pass phrase, at least 12 characters long as activation data for the private key.
TR-GRID CA private key is protected by a passphrase of at least 15 characters.

6.4.2 Activation Data Protection

The TR-GRID CA does not have access to or generate the private keys of a subscriber. The key pair is generated and managed by the client and it is subscriber's responsibility to keep the private key secure.
The passphrase for the private key of CA root certificate is kept separately in paper form with an access limited to CA personnel.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

- The operating systems of CA/RA servers are protected at a high degree of security by applying all the relevant patches.
- To discover invalid software applications, monitoring is used.
- System configuration is reduced to minimum.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

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

6.8 Time Stamping

No stipulation.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3

7.1.2 Certificate Extensions

TR-GRID CA supports and uses the following X.509 v3 Certificate extensions:

- CA root certificate extensions:
  - Basic Constraints: critical, CA:TRUE
  - Key Usage: critical, CRL Sign, Key Cert Sign
  - Subject Key Identifier
  - Authority Key Identifier
  - CRL Distribution Points

- End entity certificate extensions for users:
  - Basic Constraints: critical, CA:FALSE
  - Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment
  - Extended Key Usage: TLS Web Client Authentication, E-mail Protection
  - CRL Distribution Points
  - Authority Key Identifier
  - Subject Key Identifier
  - Certificate Policies
  - Subject Alternative Name: Email=e-mail address of user, optional

- End entity certificate extensions for hosts:
  - Basic Constraints: critical, CA:FALSE
  - Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment
  - Extended Key Usage: TLS Web Client Authentication, TLS Web Server Authentication
  - CRL Distribution Points
  - Authority Key Identifier
  - Subject Key Identifier
  - Certificate Policies
  - Subject Alternative Name: DNS Name=FQDN for hosts

7.1.3 Algorithm Object Identifiers

The following hash/digest algorithm is used:

- Secure Hash Algorithm-1 (x500 oid:1.3.14.3.2.26)

The following signature algorithm is used:

- RSA (x500 oid: 1.2.840.113549.1.1.1)

7.1.4 Name Forms

See section 3.1.1.

7.1.5 Name Constraints

See section 3.1.2.

7.1.6 Certificate Policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs are in X.509 v2 format, compliant with RFC 3280. SHA1 algorithm is used to generate CRLs.

7.2.2 CRL and CRL Entry Extensions

The CRL extension Authority Key Identifier and CRL Number will be used in CRLs.

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

TR-GRID CA accepts being audited by other accredited CAs to verify its adherence to the rules and procedures specified in its CP/CPS document.

8.2 Identity/qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communication of Results

No stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

For any service supplied, TR-GRID CA charges no fee.

9.1.2 Certificate Access Fees

See section 9.1.1.

9.1.3 Revocation or Status Information Access Fees

See section 9.1.1.

9.1.4 Fees for Other Services

See section 9.1.1.

9.1.5 Refund Policy

See section 9.1.1.

9.2 Financial Responsibility

TR-GRID CA rejects any financial or any other sort of responsibility for damages arising from its operations.

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-entities

Not applicable.

9.3 Confidentiality of Business Information

No stipulation.

9.3.1 Scope of Confidential Information

Not applicable.

9.3.2 Information not within the Scope of Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Confidential Information

Not applicable.

9.4 Privacy of Personal Information

TR-GRID CA does not collect any confidential or private information except for the case when CA or RA archives copies of ID documents for identity validation of a user certificate request. TR-GRID CA guarantees that this personal information will not be used for any other purposes.

9.4.1 Privacy Plan

See section 9.4.

9.4.2 Information Treated as Private

See section 9.4.

9.4.3 Information not Deemed Private

Information stated in issued certificates and CRLs is not considered to be confidential. TR-GRID CA collects the following information, which is not deemed as private, from the subscriber:

- Organizational e-mail address
- Name and surname

- Organization

9.4.4 Responsibility to Protect Private Information

See section 9.4.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Parts of this document are inspired by:

- RFC 2527
- RFC 3647
- Cern CA Policy
- Grid Canada CP/CPS
- HellasGrid CA CP/CPS

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

No stipulation.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

Based on this document, TR-GRID CA accepts neither explicit nor implicit liability for its actions.

TR-GRID CA does not guarantee the security or appropriateness of a service that is identified by a TR-GRID certificate. The certification service is run with an optimum level of security and it tries to supply the best-effort conditions. It assures its procedures described in this document, but it will take no responsibility for the improper use of the issued certificates.

TR-GRID CA rejects any financial or any other sort of responsibility for damages arising from its operations.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Subscribers will not be informed in advance if the CP / CPS document is changed. Changes are announced to EUGridPMA and get approved before the new CP/CPS is declared on the website as defined in section 2.3. Changes are published on the website as well.

9.12.2 Notification Mechanism and Period

See section 9.12.1.

9.12.3 Circumstances under which OID must be Changed

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

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

Applicability, interpretation, construction and validity of this document must be treated according to Turkish Republic laws.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

No stipulation.

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.17 Other Provisions

No stipulation.