TR-GRID

CERTIFICATION AUTHORITY

CERTIFICATE POLICY

AND

CERTIFICATION PRACTICE STATEMENT

Version 1.0

June, 2005

Table of Contents

1. INTRODUCTION

1.1 Overview

This document is organized according to the specifications proposed by the RFC 2527. 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.

1.2 Identification

Document Title

TR-GRID CA Certificate Policy and Certification Practice Statement

Document Version

1.0

Document Date

June 20, 2005

ASN.1 Object Identifier (OID)

1.3.6.1.4.1.23658.10.1.1.0

1.3 Community and Applicability

TR-GRID CA provides PKI services to the Turkish academics and research communities who participate in national or international Grid activities.

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 End Entities

TR-GRID CA issues certificates to the following entities:

- TR-GRID users (people)
- TR-GRID computers (hosts)
- TR-GRID services (host applications)

1.3.4 Applicability

User certificates can be used to authenticate a user that would like to benefit from the Grid resources.

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

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

1.4 Contact Details

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

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

Asli Zengin
Phone: +90 312 2989367
E-mail: asli@ulakbim.gov.tr

Address: YOK Binasi B5 Blok 06539
Bilkent, Ankara
Turkey
Website: http://www.grid.org.tr/ca

2. GENERAL PROVISIONS

2.1.1 CA Obligations

The TR-GRID CA is entirely responsible for the following subjects:

- considering certificate requests and issuing new certificates
- publication of certificates
- revocation of the invalid certificates
- periodical publication of Certificate Revocation Lists (CRLs)

- procedures related to certificate renewals
- ensuring that all CA activities are performed under the rules and procedures specified in this document

2.1.2 RA Obligations

TR-GRID RAs must sign an agreement to adhere to the Certificate Policy referred in this document with the following responsibilities:

- application/registration procedure for the applicant
- identification of the applicant
- authentication of the applicant
- secure communication with CA by signed e-mails, SSL protected private web pages and voice conversations with a known person

2.1.3 Subscriber Obligations

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 2.2
- admission of statements about confidentiality of information emphasized in section 2.8
- 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

2.1.4 Relying Party Obligations

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

2.1.5 Repository Obligations

TR-GRID CA will provide on-line access to any information related to TR-GRID CA with a periodical update of CRLs on its website http://www.grid.org.tr/ca

2.2 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.

2.3 Financial Responsibility

As stated in section 2.2, no financial responsibility is accepted with respect to the use or management of any issued certificate.

2.4 Interpretation and Enforcement

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

2.5 Fees

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

2.6 Publication and Repositories

2.6.1 Publication of CA Information

TR-GRID CA will maintain a secure on-line repository that includes:

- The TR-GRID CA root certificate
- User and host certificates issued by the CA
- A periodically updated Certificate Revocation List (CRL)
- All versions (current and past) of its verified CP/CPS document

- Other information that can be regarded as relevant to TR-GRID CA

2.6.2 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.

2.6.3 Access Controls

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.

2.6.4 Repositories

The repository of certificates and CRLs are available at http://www.grid.org.tr/ca

2.7 Compliance Audit

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.

2.8 Confidentiality

TR-GRID CA requests subscribers' full names and e-mail addresses. This information is used to form unique and meaningful subject names in the issued certificates.

Information stated in issued certificates and CRLs is not considered to be confidential. The TR-GRID CA does not require any kind of confidential information.

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.

2.9 Intellectual Property Rights

Parts of this document are inspired by:

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

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 Meaningful Name Specification

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).

3.1.3 Uniqueness of a Name

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.

3.1.4 Authentication of Organization

Not yet assigned.

3.1.5 Authentication of an 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.

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 Routine Rekey

Expiration warnings will be sent to subscribers before it is rekey time. Rekey before expiration can be executed by stating a rekey request signed with the personal certificate of the subscriber. Rekey after expiration uses completely the same authentication procedure as new certificate.

3.3 Rekey after Revocation

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

3.4 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 3.1.5

4. OPERATIONAL REQUIREMENTS

4.1 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.
- User certificate requests must be submitted via SSL protected HTTP transport.

4.2 Certificate Issuance

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.

4.3 Certificate Acceptance

No specification.

4.4 Certificate Suspension and Revocation

4.4.1 Revocation Circumstances

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.

4.4.2 Persons that 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.

4.4.3 Procedure of 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.

4.4.4 Circumstance of Certificate Suspension

No specification.

4.4.5 CRL Issuance Frequency

See section 2.6.2

4.4.6 CRL Checking Requirements

A relying party must verify the certificate that it uses considering the most recently issued CRL.

4.4.7 On line Revocation/Status Checking Availability

At present, no on line service for this purpose is available.

4.5 Security Audit Procedures

Before the records archival, all system boots and shutdowns, system logins / logout are audited.

4.6 Records Archival

4.6.1 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

4.6.2 Retention Period for Archive

Minimum retention period is three years.

4.6.3 Protection of Archive

Archives are kept in a separate room with limited access.

4.7 Key Changeover

The CA's private key is changed periodically; from that time on, the new key will be valid in order to sign new certificates or CRL lists of new certificates. The overlap of the old and new key must be at least one year. 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.

4.8 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.

4.9 CA 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

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1.1 Site Location

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 specification.

5.1.4 Water Exposures

No specification.

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 specification.

5.1.8 Off-site Backup

No specification.

5.2 Procedural Controls

No specification.

5.3 Personnel Controls

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

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 Entity

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 Users

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 specification.

6.1.7 Parameter Quality Checking

No specification.

6.1.8 Hardware/Software Key Generation

Key generation is performed by OpenSSL software.

6.1.9 Key Usage Purposes

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

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

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 specification.

6.2.3 Private Key Escrow

Not specified yet.

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, floppy disks and CD-ROMs. The password for the private key is kept separately in paper form with an access control. Only, authorized CA personnel has access to the backups.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the Public and Private Keys

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

6.4 Activation Data

TR-GRID CA private key is protected by a passphrase of at least 15 characters.

6.5 Computer Security Controls

6.5.1 Specific Technical Requirements for Security

- 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 specification.

6.6 Life Cycle Technical Controls

No specification.

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 Cryptographic Module Engineering Controls

No specification.

7. CERTIFICATE AND CRL 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

- End entity certificate extensions
  - Basic Constraints: critical, CA:FALSE
  - Key Usage: critical, Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
  - Subject Key Identifier
  - Authority Key Identifier
  - Subject Alternative Name: subscriber's e-mail address, IP address and/or DNS Name=FQDN for hosts
  - Issuer Alternative Name
  - CRL Distribution Points
  - Certificate Policies
  - Netscape Base URL
  - Netscape Cert Type: server, client, e-mail

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 specification.

7.1.8 Policy Qualifiers Syntax and Semantics

No specification.

7.2 CRL Profile

7.2.1 Version Number

X.509 v1

7.2.2 CRL and CRL Entry Extensions

No specification.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

Subscribers will not be informed in advance if the CP / CPS document is changed. Changes are declared on the website as defined in section 2.6.

8.2 Publication and Notification Policies

This policy document and the forthcoming new versions will be available on line on the website www.grid.org.tr/ca

8.3 CPS Approval Procedures

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

9. GLOSSARY

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.