Research unit of Technologies
of Information and Communication

Tunisian National Grid

TNGrid CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Draft_VERSION 1.0

Document OID: 1.3.6.1.4.1.37660.1.1.1.0

July 2011

Table of Contents

1 INTRODUCTION

1.1 Overview

The TNGrid project is an initiative of the research unit of Technologies of Information and Communication (UTIC) at Ecole Supérieure des Sciences et Techniques de Tunis (ESSTT) of the University of Tunis, to set up a Grid infrastructure and Grid computing.

This document is the combined Certificate Policy and Certification Practice Statement of the TNGrid Certification Authority. It describes the set of procedures followed by the TNGrid CA and is structured according to RFC 3647.

1.2 Document name and identification

Title: TNGrid CA Certificate Policy (CP) and Certification Practice Statement (CPS)

Version: 1.0 (Draft)

Date: July 2011

Expiration: This document is valid until further notice.

OID assigned: 1.3.6.1.4.1.37660.1.1.1.0

OID structure:

- IANA: 1.3.6.1.4.1
- iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)
- UTIC: 37660
- TNGrid CA: 1
- This CP/CPS document: 1
- Version of this CP/CPS: 1.0

1.3 PKI participants

1.3.1 Certification authorities

The TNGrid CA doesn't issue certificates to subordinate Certification Authorities.

1.3.2 Registration authorities

The procedures of identification and authentication of the certificate applicants are performed by trusted individuals (Registration Authorities RAs), appointed by the TNGrid CA. At any time the current list of valid RAs will be available in an on-line repository operated by the TNGrid CA.

1.3.3 Subscribers

In the context of this CP/CPS the term “Subscribers” eligible for certification from the TNGrid CA are:

- Individuals from organizations involved in the TNGrid
- Servers/hosts operated by members of TNGrid
- Services running on servers which are used in activities of TNGrid

1.3.4 Relying parties

Users of Grid computing infrastructures that are using the public keys, in certificate issued by the TNGrid 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

Certificates issued by the TNGrid CA are only valid in the context of scientific activities:

- User certificates can be issued to authenticate the users who benefit from academic and research resources, services and activities.
- Host certificates can be used for the machines of clusters inside TNGrid
- Service certificates can be used to recognize services used inside TNGrid

1.4.2 Prohibited certificate uses

Any other kind of usage such as financial transactions is strictly forbidden.
Using certificates for purposes contrary to Tunisian law is explicitly prohibited.

1.5 Policy administration

1.5.1 Organisation administering the document

UTIC research unit is responsible for the management, registration, maintenance and interpretation of TNGrid CA. It is reachable at:

ESSTT, UTIC
5 Avenue Taha Hussein, BP, 56, Bâb Manara, 1008
Tunis, Tunisia

Home page: http://www.utic.rnu.tn
TNGrid CA: http://www.tngrid.tn/index/ca
E-mail: ca@tngrid.tn
Phone: +216 97 41 93 28
Fax: +216 71 39 11 66

1.5.2 Contact person

The contact persons for questions about this document or any other TNGrid CA related issues is:

Mohamed Jemni
ESSTT, UTIC
5 Avenue Taha Hussein, BP, 56, Bâb Manara, 1008
Tunis, Tunisia
e-mail: mohamed.jemni@fst.rnu.tn
Phone: +216 97 41 93 28
Fax: +216 71 39 11 66

Deputy contact:

Heithem Abbes
ESSTT, UTIC
5 Avenue Taha Hussein, BP, 56, Bâb Manara, 1008
Tunis, Tunisia
e-mail: heithem.abbes@esstt.rnu.tn
Phone: +216 98 47 52 15
Fax: +216 71 39 11 66

1.5.3 Person determining CPS suitability for the policy

Mohamed Jemni
ESSTT, UTIC
5 Avenue Taha Hussein, BP, 56, Bâb Manara, 1008
Tunis, Tunisia
e-mail: mohamed.jemni@fst.rnu.tn
Phone: +216 97 41 93 28
Fax: +216 71 39 11 66

Heithem Abbes
ESSTT, UTIC
5 Avenue Taha Hussein, BP, 56, Bâb Manara, 1008
Tunis, Tunisia
e-mail: heithem.abbes@esstt.rnu.tn
Phone: +216 98 47 52 15
Fax: +216 71 39 11 66

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

Authentication: The process of establishing that individuals or organizations are who they claim to be. This process corresponds to the second process involved in identification.

Certificate Policy (CP): 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. 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.

Certificate Revocation List (CRL): A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

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.

End Entity (EE): Subscribers (users, hosts and services) of the TNGrid CA.

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The repository of certificates and CRLs are available at http://www.tngrid.tn/index/ca/.

2.2 Publication of certification information

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

- The TNGrid 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
- E-mail addresses for inquiries and fault reporting
- Mailing address of CA administration location
- Other information that can be regarded as relevant to TNGrid CA

2.3 Time or frequency of publication

Certificates will be put to the TNGrid CA website as soon as they are issued.

CRL publication will be updated as described is section 4.9.7.

New versions of all TNGrid 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 controls on repositories

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

TNGrid CA does not impose any access control restrictions to the information available at its website, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS.

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:

- in case of user certificate the subject name must include the person name in the CN field;
- in case of host certificate the subject name must include the FQDN in the CN field;

- in case of service certificate the subject name must include the FQDN of the service server name in the CN field.

The common names must be encoded as Printable Strings according with RFC 1778 and RFC 2252. The characters allowed in the common names of personal certificates are as follows:

- ‘ ’ (space), ‘(’, ‘)’ and ‘-’;
- ‘0’ – ‘9’;
- ‘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 section 3.1.1). The name must not refer to a role. Subscribers can neither be anonymous nor pseudonymous.

For host certificates, the CN must be stated as the fully qualified domain name (FQDN) of the host.

3.1.3 Anonymity or pseudonymity of subscribers

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

3.1.4 Rules for interpreting various name forms

The CN component of the subject name in a certificate for a user must contain the first and the family name as it appears in the authentication document proving the name of the subscriber.

The CN entry for a host must be the fully qualified domain name (FQDN) that can be universally used to access that host.

The CN entry for a service must be the FQDN of the service server name.

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 TNGrid 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 private key

For user certificates, requests can be submitted in one way:

- User certificate requests can be submitted by an online procedure on TNGrid CA secure website (http://www.tngrid.tn/index/ca), using a web browser. The key pairs are generated by the web browser locally on the machine. The certificate (public key signed by the CA) can only be downloaded using the same browser, including the key pair, on the same machine, by a secure URL on TNGrid CA website.

For host or service certificates, requests can be submitted in one way:

- The host or service administrator creates key pair and certificate request file in PKCS#10 format using OpenSSL package, submit certificate request file to the TNGrid CA secure website (http://www.tngrid.tn/index/ca). The private key is kept by the host or service administrator. The certificate can be downloaded using a browser by a secure URL on the TNGrid CA website.

3.2.2 Authentication of organization identity

No stipulation.

3.2.3 Authentication of individual identity

The subject must contact personally the nearby RA in order to verify his identity and the validity of the request. The subject authentication is performed through the presentation of a valid Tunisian ID document or passport.

The RA shall send via a secure communication channel or in a signed e-mail to the TNGrid CA the following information:

- 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.

Host certificates can only be requested by the administrator responsible for the particular host. The host administrator must already have a valid personal TNGrid CA certificate, required to authenticate to TNGrid CA secure website and request host certificate.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

The requester provides documentation for the organizational name that should be included in the certificate. The wording of the organizational name that should be included in the certificate needs to be identical to the wording in the documentation provided.

3.2.6 Criteria for 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 issued to subscribers when re-key time arrives. Re-key before expiration can be accomplished by sending a re-key e-mail request signed with the current user certificate. Re-key after expiration follows the same authentication procedure as new certificate. After 5 years face to face identity validation is required as described in 3.2.3.

3.3.2 Identification and authentication for re-key after revocation

A revoked certificate cannot be renewed; user has to request a new certificate. The authentication of a new certificate request follows the rules specified in section 3.2.3.

3.4 Identification and authentication for revocation request

Certificate revocation requests should be submitted via e-mail. In case the revocation request is for a user certificate, the e-mail must be signed by the private key corresponding to the certificate that is requested to be revoked, which must be a valid, non-expired, non-revoked TNGrid CA certificate.

If the revocation request is for a host or service certificate: the e-mail must be signed by the private key corresponding to the certificate of the person responsible of the host or service. When e-mail is not an option, the request will be authenticated using the procedure described in section 4.9.3.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

The TNGrid CA issues certificates to eligible organizations, i.e. entities that are connected to the academic and research network RNU, for:

- users affiliated to eligible organization for which they take full responsibility,
- hosts administered by the requesting eligible organization, and
- services provided on a host that is administered by an eligible organization.

4.1.2 Enrollment process and responsibilities

- For user certificates, request can be submitted as follow:

User certificate requests is submitted by an online procedure on TNGrid CA secure website (http://www.tngrid.tn/index/ca/), using a web browser. The key pairs are generated by the web browser locally on the user's machine.

The certificate (public key signed by the CA) can only be downloaded using the same browser, including the key pair, on the same machine, by a secure URL from TNGrid CA website.

- For host or service certificates, requests can be submitted as follow:

The host or service administrator creates key pair and certificate request file using *OpenSSL* packages, submit certificate request file to the TNGrid CA by signed e-mail. The private key is kept by the host or service administrator. The certificate request will be verified by the appropriate RA, who will approve or disapprove the request according to sections 4.2.1 and 4.2.2. If the request is approved by the RA, the requester will then receive an e-mail, containing his/her certificate or information needed to download using a browser by a secure URL on the TNGrid CA website.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

In all the other cases (re key of user certificate while current certificate is valid, request for host or service certificate) the authentication of the certificate application will take place by checking that the requester has a valid TNGrid CA certificate. Upon successful authentication, the certificate application will be forwarded to the RA in order to validate the information included in the certificate request.

4.2.2 Approval or rejection of certificate applications

In order to approve any certificate application request, the following conditions must be filled:

1. the certificate application must be authenticated first by the RA as described in section 4.2.1;
2. the subject must apply the certificate request within 2 working days after the successful authentication performed by the RA;
3. the subject must be an acceptable subscriber entity, as defined by this Policy;
4. the request must obey the TNGrid CA distinguished name scheme;
5. the distinguished name must be unambiguous and unique;
6. the key must have at least 2048 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. Through a secured web interface (with https), RA sends approval and validation decisions to CA.

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

The certificate request shall be transferred to the computer which holds the private key of TNGrid CA and which is a dedicated machine and not connected to any network. On this system the certificate is created and signed. The signed certificate shall then be transferred back to the online CA server and an email will be sent to the relevant RA manager informing him/her about the action.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The TNGrid CA may notify the requester in different ways:

- E-mail the certificate directly to the subscriber
- E-mail information permitting the subscriber to download the certificate from a web site or repository

In the same e-mail the subscriber will be requested to return an e-mail signed by his/her newly issued certificate, in which he/she will be stating that he/she accepts certificate signed by TNGrid CA and that she/he adheres to this policy.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber must send an e-mail within 15 days from the day that his/her certificate was issued. He/she will sign his/her e-mail with issued certificate confirming the acceptance of the certificated his/her adhesion to the policy. He/she assumes the responsibility to notify the TNGrid CA immediately:

- In case of possible private key compromise
- When the certificate in no longer required
- When the information in the certificate becomes invalid

4.4.2 Publication of the certificate by the CA

Upon receipt of a certificate acceptance the TNGrid CA will make available the certificate on its repository.

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers may use their certificate as stated in section 1.4. They shall:

- Use certificate issued by TNGrid CA exclusively for legal and authorized intended purposes
- Only use certificate issued by TNGrid CA on behalf of the person, entity, or organization listed as the subject of such a certificate

The subscriber must discontinue use of the private key along with the certificate following the expiration or revocation of the certificate.

The end entity certificates and their private keys must not be shared by the users or hosts/server administrators.

4.5.2 Relying party public key and certificate usage

Relying party shall:

- Be held responsible to understand the proper use of certificates
- Read and agree to all terms and conditions of this CP/CPS
- Verify the validity of the certificate by consulting the TNGrid CA CRL

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.2 Who may request renewal

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.3 Processing certificate renewal requests

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.4 Notification of new certificate issuance to subscriber

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.5 Conduct constituting acceptance of the renewal certificate

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.6 Publication of the renewal certificate by the CA

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.7 Notification of certificate issuance by the CA to other entities

TNGrid CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Subscribers must regenerate their key pair in the following cases:

- The certificate is revoked
- The certificate has expired
- The subscriber need to do change in the certificate parameter

4.7.2 Who may request certification of a new public key

The owner of a valid certificate may request the certification of a new public key for the cases listed in section 4.7.1. If the certificate has already expired, a certificate request procedure as described for an initial certification request must be followed.

4.7.3 Processing certificate re-keying requests

Upon receipt of the request endorsed by the appropriate RA, the TNGrid CA will process the re-keying as it processes an initial certification request. The main exception is that the documentation which is valid and present at the RA does not need to be represented when requesting a new certificate through re-keying.

4.7.4 Notification of new certificate issuance to subscriber

The same procedure will be followed as described in section 4.3.2

4.7.5 Conduct constituting acceptance of the re-keyed certificate

The same procedure will be followed as described in section 4.4.1

4.7.6 Publication of the re-keyed certificate by the CA

The same procedure will be followed as described in section 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

The same procedure will be followed as described in section 4.4.3

4.8 Certificate modification

Certificates must not be modified. In case of changes, the old certificate must be revoked, and new certificate with new key pair must be requested as described in section 4.1.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certification 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 the 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

The certificate must be revoked without delay by the TNGrid CA if:

- The private key of subscriber has been lost, compromised and/or misused in any other manner
- The certificate contains data that is no longer valid
- The certificate is not needed any more
- The subscriber does not comply with the terms and conditions of this CP/CPS
- Service and host certificates are retired

4.9.2 Who can request revocation

The revocation of the certificate can be requested by:

- The certificate owner
- The TNGrid CA
- The appropriate RA
- The organisation/unit that wants to revoke its consent
- Any other entity presenting proof of knowledge of the private key compromise

4.9.3 Procedure for revocation request

A revocation request must be made by the following cases:

- The subscriber send an e-mail signed with the private key certificate associated with the (still not expired) certificate.

- On behalf of the organisation/unit that consented to the certificate in an e-mail signed by an authorized person.

If no such e-mail can be sent, the revocation can be initiated via oral communication with the appropriate RA or the TNGrid CA. Authentication will be performed with the same procedure as described in section 3.2.2 and section 3.2.3.

The TNGrid CA informs the owner of a newly revoked certificate and the appropriate RA of the issued revocation.

4.9.4 Revocation request grace period

All revocation requests shall be issued and executed without delay.

4.9.5 Time within which CA must process the revocation request

The TNGrid CA will process a certificate revocation request with highest priority during one working day.

4.9.6 Revocation checking requirement for relying parties

The relaying party must verify the validity of the certificate by consulting the TNGrid CA CRL in effect at the time of use of the certificate.

4.9.7 CRL issuance frequency (if applicable)

CRL will be published in the on-line repository as soon as issued and at least once every 23 days. The maximum CRL lifetime is 30 days; and CRL are issued at least 7 days before expiration. CRL publication will be updated immediately after a revocation is issued.

4.9.8 Maximum latency for CRLs (if applicable)

The CRL will be transferred from the off-line CA system after creation without delay to the on-line repository.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

There is no online revocation checking service, but a relying party must verify a certificate against the most recent CRL issued in order to validate the use of the certificate.

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

TNGrid CA does not suspend certificates.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

TNGrid CA provides certificates and certificate status services through its website. All valid certificates and the most up-to-date CRL are available in the same repository.

4.10.2 Service availability

The TNGrid CA website is maintained on best effort basis with intended availability of 24x7. Due to unavoidable maintenance activities and the nature of the Internet this service can't be guaranteed to be always accessible.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The term of the contractual relationship is given by the end of period of validity as indicated in the certificate. A subscription may end earlier if the subscriber requests it or if the organizational unit which he/she belongs asks for it.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No key escrow or recovery services are provided.

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

5.1.1 Site location and construction

The TNGrid CA operates in controlled UTIC Grid Center, in the Ecole Supérieure des Sciences et Techniques de Tunis (ESSTT) where the details of address are in section 1.5.1.

5.1.2 Physical access

Physical access is only granted to authorized personnel of the TNGrid CA.

5.1.3 Power and air conditioning

TNGrid CA equipment is protected by uninterrupted power supplies and the UTIC Grid Center is properly air-conditioned.

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

The TNGrid CA private key (see section 6.2.4) and backup copies of CA related information are stored in removable storage media. Removable media are kept in locked safe places to which only authorized personnel have access.

5.1.7 Waste disposal

Waste containing potential confidential data must be physically destroyed before being trashed.

5.1.8 Off-site backup

No off-site backup is currently performed.

5.2 Procedural Controls

5.2.1 Trusted role

Personnel which include system and network administrators, operators and executives who are designed to oversee the CA's operations shall, for purpose of this policy, be considered as serving in a trusted role.

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

The role of the TNGrid CA requires experienced personnel who are technically and professionally competent.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to TNGrid CA and RA operators.

5.3.4 Retraining frequency and requirements

TNGrid CA will perform operational audit of the CA/RA staff at least once per year. If the results of the operational audit are not satisfactory, retraining will be considered.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Documentation regarding all the operational procedures of the TNGrid CA is supplied to personnel for successfully performing their task.

5.4 Audit logging procedures

5.4.1 Types of event recorded

Certificate management functions:

- Certificate request
- Revocation request
- Certificate download/installation
- CRL issuing
- All issued certificates

System management functions:

- Boot/reboot and shutdown
- Login/logout
- Backup and restore the CA database

5.4.2 Frequency of processing log

The log is automatically archived to a file when 100% full relating to the file size.
The log files shall be reviewed once a month and analyzed following an alarm or anomalous event.

5.4.3 Retention period for audit log

Audit logs will be retained for a period of minimum three years.

5.4.4 Protection of audit log

Only authorized TNGrid CA personnel are allowed to view and process audit logs. Audit logs are copied to an off line medium.

5.4.5 Audit log backup procedures

Audit logs are copied to an off line medium which is stored is safe place.

5.4.6 Audit collection system (internal vs external)

The audit collection system is internal to TNGrid CA.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records Archival

5.5.1 Types of records archived

The following records archived are:

- Certification and revocation requests
- Issued certificates
- Issued CRLs
- All e-mail messages sent to or send by TNGrid CA
- All audit logs as described in 5.4.1
- All identity documents which are collected for user authentication

5.5.2 Retention period for archive

The minimum retention period is three years.

5.5.3 Protection of archive

Only authorized CA personnel are allowed to view and process records archived. All records archive are stored on off line medium.

5.5.4 Archive backup procedures

All records archive are kept on off line medium which is stored in safe place.

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 TNGrid CA.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The CA's private signing key is changed periodically; from that time only the new key will be used for certificate signing purposes. The overlap of the old and new key will be at least 1 year. For this overlapping period, the older but still valid certificate along with the corresponding private key will be available in order to verify digital signatures and issue CRLs.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

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

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 needed, the TNGrid CA private key stored in external media will be restored according restore procedures (see section 6.2.4), therefore operations should restart without need to revoke all issued certificates.

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

No stipulation.

5.8 CA or RA Termination

Before the TNGrid CA terminates its services, it will;

- Inform the RAs, subscribers and relying parties as soon as possible,
- Announce CA termination as widely as possible,
- Stop issuing and distributing certificates,
- Revoke all certificates,
- Generate and publish last CRL and CRL signing,
- Destroy all copies of TNGrid CA private keys.

CA executive manager at termination will be responsible for the subsequent archival of all records as required is section 5.5.2.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The key pair of the TNGrid CA is generated by authorized CA staff on the offline CA server using OpenSSL packages. Each subscriber (including RA agents) must generate his/her own key pair. TNGrid CA does not generate private keys on behalf of subscribers.

6.1.2 Private key delivery to subscriber

The TNGrid CA does not generate private key for its subscribers therefore does not deliver private keys to them.

6.1.3 Public key delivery to certificate issuer

The subscriber's public key must be transferred to the TNGrid CA in a secure manner: by online transaction from a secure web server for personal certificates or by signed e-mail for server and service certificates.

6.1.4 CA public key delivery to relying parties

The TNGrid CA certificate can be downloaded from the TNGrid CA web site.

6.1.5 Key sizes

The TNGrid CA key is an RSA key with a size of 2048 bits.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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 a subscriber certificate for:

- Authentication
- Data and key encipherment
- Message integrity
- Session establishment

With an RA certificate for:

- All activities needed for the work of an RA agent

With the CA certificate for:

- Certificates signing
- CRLs signing

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

6.2 Private Key Protection and Cryptographic Module Engineering

6.2.1 Cryptographic module standards and controls

End entities shall use the web form available in on the TNGrid CA web site for key generation.

The CA private key is generated using OpenSSL.

CA operator shall have his/her personnel copy of the CA privates key encrypted with a passphrase of at least 15 characters. These encrypted private key should be stored on the offline TNGrid CA computer.

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

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 that is accessible for only authorized CA operators.

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 cryptographic module

TNGrid CA does not use cryptographic module.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

TNGrid 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

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

6.2.10 Method of destroying private key

Private key backup copies will be disposed by physical destruction of the media.

6.2.11 Cryptographic module rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate operational periods and key pair usage periods

The default subscriber certificate lifetime is one year. The lifetime of the TNGrid CA root certificate is 20 years.

6.4 Activation Data

6.4.1 Activation data generation and installation

TNGrid does not generate activation data for subscribers. It's upon the subscriber to generate a secure passphrase in order to be used as activation data for his/her private key.

The passphrase used to activate the TNGrid CA private key is generated on the computer used for the CA signing operations and must be at least 15 characters long.

6.4.2 Activation data protection

The TNGrid CA does not have access to or generate the private keys of a subscriber. The key pair is generated and managed by the subscriber and it is subscriber's responsibility to keep the private key secure.

The passphrase for the private key of TNGrid 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

TNGrid CA servers include the following functionalities:

- The operating systems of CA/RA computers are maintained at high level of security by applying all recommended and applicable security patches
- Monitoring is performed to detect unauthorized software changes
- Services is reduced to the bare minimum
- Machines used for RA are protected by a suitably configured firewall
- The dedicated machine used for signing certificates isn’t connected to any kind of networks

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

The signing machine is kept offline and dedicated for the CA operations. All other CA machines are protected by a firewall and/or by removing all unnecessary services.

6.8 Time stamping

All time stamping of entries created on the online servers at the TNGrid CA is based on the network time provided by the time server of the RNU (National and Research Network of Tunisia).

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by the TNGrid CA.

7.1.2 Certificate extensions

For user certificates:

- Basic Constraints: critical, ca: false
- Subject Key Identifier: hash
- Authority Key Identifier: keyid, DirName, serial
- Key Usage: critical, digitalSignature, keyEncipherment, 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, DirName, serial
- Key Usage: critical, digitalSignature, keyEncipherment, dataEncipherment
- Extended Key Usage: serverAuth, clientAuth
- CRL Distribution Points: URI
- Certificate Policies: OID

- Subject alternative name: Server's DNS FQDN host name

For CA certificate:

- Basic Constraints: critical, ca: true
- Subject Key Identifier: hash
- Authority Key Identifier: keyid, DirName, serial
- Key Usage: critical, KeyCertSign, cRLSign
- CRL Distribution Points: URI

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures for certificates issued by the TNGrid CA are according to:

- Hash Function: id-sha1 1.3.14.3.2.26
- RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
- Signature Algorithm: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name forms

The DN of the TNGrid CA certificate issuer must be:

C=TN/O=TNGrid/CN=TNGrid CA

Depending on the type of entity the DN has the following form:

- ***C=TN***
- ***O=TNGrid***
- *OU*=Unit: This entry may be used recursively
  - Each organization may define the hierarchy to be used, the first entry denotes the organization to which the entity belongs
  - For an RA the last OU must be *Registration Authority*
- *L*= Locality Name: The structure where the RA is appointed
- *CN*= common name: Depending on the type of the entity the CN must be:
  - For personal certificate: the first name and last name (optionally an extension to make the name unique within the organizational unit)
  - For host: the Fully Qualified Domain Name FQDN
  - For service: the FQDN of the host it is running on

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy Object Identifier

The OID of this CP/CPS is: **1.3.6.1.4.1.37660.1.1.1.0**

Each certificate must reference a policy OID, and may contain several as long as none of the policy constraints conflict. The extension certificate Policy is the OID of this document (1.3.6.1.4.37660.1.1.1.0) and the OID of the Classic X.509 Profile versions 4.x (1.2.840.113612.5.2.2.1.4)

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 TNGrid CA must create and publish X.509 version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The TNGrid CA will issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation will not be included in the individual CRL entries.

The CRL must include the date by which the next CRL will be issued. A new CRL must be issued before this date if new revocations are issued.

The CRL extensions that must be included are:

- the authority key identifier
- the CRL number

No other CRL entry extensions will be used.

7.3 OCSP profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and circumstances of assessments

TNGrid 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.

TNGrid CA accepts being audited by other accredited CAs to verify it’s 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

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 result of deficiency

The TNGrid CA must take immediate action if the assessment reveals a deficiency related to provisions of the CP/CPS document. 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 should be revoked immediately.

8.6 Communication of result

The TNGrid CA staff will make the result publicly available on the TNGrid CA website.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

For any service supplied, no fees will be charged by TNGrid CA.

9.1.1 Certificate issuance or renewal fees

See section 9.1.

9.1.2 Certificate access fees

See section 9.1.

9.1.3 Revocation or status information access fees

See section 9.1.

9.1.4 Fees for other services

See section 9.1.

9.1.5 Refund policy

See section 9.1.

9.2 Financial responsibility

TNGrid CA denies any financial responsibility for any damages resulting from use of 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

TNGrid 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. TNGrid CA guarantees that this personal information will not be used for any other purposes.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

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

- Subscriber's name,
- Subscriber's e-mail address,
- Subscriber's organization,
- Subscriber's certificate.

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 3647
- CERN CA Policy
- SEE-GRID CP/CPS
- SWITCH CP/CPS
- INFN CP/CPS
- AUSTRIANGRID CP/CPS
- UK e-Science CP
- Grid Canada 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, TNGrid CA accepts neither explicit nor implicit liability for its actions.

TNGrid CA does not guarantee the security or appropriateness of a service that is identified by a TNGrid 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.

TNGrid 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

This document become effective after its publication on the website of TNGrid CA starting at the date announced there. No term is 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 participant

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendments

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see section 1.5.4).

9.12.2 Notification mechanism and period

The amended CP/CPS document shall be published on TNGrid CA Web pages at least 2 weeks before it becomes effective. TNGrid 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 TNGrid CA and submitted to EUGridPMA.

9.13 Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the manager of TNGrid CA.

9.14 Governing law

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

9.15 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of a TNGrid CA certificate must comply with the Tunisian law. Activities initiated from or destined for another country than Tunisia 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 section 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 provisions.

9.16.5 Force Majeure

Events that are outside the control of the TNGrid CA will be dealt with immediately by the EUGridPMA.

9.17 Other provisions

No stipulation.