NG TECHNOLOGIES

Building Trust with **Next Generation** Technologies …

NG Technologies Remote Trust Services

Certification Practice Statement of NG Technologies Root Certification Authority

Identifier	PKI-CPS-ROOT-CA
Version	1.1
Description	Certification Practice Statement of NG Technologies Root CA.
Classification	Public
Approval	CEO

www.ng-sign.com
contact@ng-sign.com

Historical

Dated	*Version*	*Author*	*Comment*	*Approved by*
09/08/2021	1.0	PKI Committee	Initial version.	CEO
13/07/2022	1.1	PKI Committee	Updated paragraph Capacities for business continuity following a disaster to specify the RTO.	CEO

INDEX

1 INTRODUCTION

This document constitutes the Certification Practices Statements (CPS) of the Primary Certification Authority of NG Technologies (referred to in the document as NG Root CA).

It is the highest-level authority within the Public Key Infrastructure (PKI) set up by NG Technologies. This PKI, named **NG Remote Trust Service** (NGRTS), is made up of this Root Certification Authority to which specialized Sub Certification Authorities are attached.

The CP and CPS documents can be found at https://www.ng-cert.com/repository/public/ or http://www.ng-sign.com/repository/public/

1.1 Overview

This CPS, associated with the Certificate Policy (CP), addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by NG Root CA. NG Root CA is operated and owned by NG Technologies.

CP and CPS incorporate the requirements of RFC 3647 and contain detailed information about specifications, certification procedures and security measures for the issuance of certificates by Certification Authorities operated by NG Technologies.

1.2 Document Name and Identification

This document is the Certification Policy (CP) of the RT CA Certification Authority operated by NG Technologies.

The root OID 2.16.788.2.1 (/Country/TN/2/1 or {joint-iso-itu-t(2) country(16) tn(788) private-sector(2) Ngtechnologies(1)}) has been registered for NG Technologies services [1]at Instance Nationale des Télécommunications (INT) as the organization representing Tunisia at the ITU.

This document is identified by the OID: **2.16.788.2.1.3**

This document is the initial version of the CPS. Any revisions will be noted in the history section above and in this section. Any change of OID will be mentioned.

1.3 PKI Participants

NG Remote Trust Service (NGRTS) means the certification and electronic signature service of NG Technologies. NG Root CA is the Root Certification Authority for the PKI managed by this service.

Further details are given in the associated CP.

[1] http://oid-info.com/get/2.16.788.2.1

1.4 Certificate Usage

Regulation of this is given in the associated CP.

1.5 Policy Management

1.5.1 Entity managing this document

The entity responsible for the development, monitoring and modification of this CP is NG Technologies via a specific committee called "PKI Committee" (PKICOM/COMPKI)). PKICOM is made up of key employees responsible for the security, operation, and maintenance of NGRTS components. PKICOM is the top-level management of the PKI with full financial and administrative authority to take all necessary decisions to operate the PKI and implement the responsibilities defined in this CP.

All actions and responsibilities amputated in this document at NG Technologies are under the responsibility of PKICOM which manages all aspects (technical, operational, administrative, etc.) related to the establishment and operation of NGRTS.

1.5.2 Point-of-contact

NG Technologies
Les orangers building, Rue Lac d'Annecy, Les Berges du Lac Étage 3, Tunis 1053
contact@ng-sign.com

1.5.3 Entity determining the compliance of practices with the CPS

NG Technologies via internal and external audits.

1.5.4 CPS compliance approval procedures

Regulation of this is given in the associated CP.

1.5.5 Modification of the CP/CPS

Modification of the CP and CPS may be affected at any time in accordance with the amendment procedures specified in the CP document.

1.5.6 Definitions and acronyms

The Glossary is given in the associated CP.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

NG Technologies publishes information relating to the service it provides at https://pki.ng-sign.com/

NG Technologies publishes the valid CP, CPS and their previous versions.

Further details are given in the associated CP.

2.2 Publication of certification information

Further details are given in the associated CP.

2.3 Time or frequency of publication

Regulation of this is given in the associated CP.

2.4 Access controls on repositories

Regulation of this is given in the associated CP.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Regulation of this is given in the associated CP.

3.2 Initial Identity Validation

This Root CA is only allowed to issue certificates to intermediate Certification Authorities operated by NG Technologies.
The information and data to be included and signed in the certificate must be specified in the key ceremony script and have already been validated by NG Technologies.

Further information is in the associated CP.

3.3 Identification and authentication for re-key requests

Regulation of this is given in the associated CP.

3.4 Identification and Authentication for Revocation Requests

Regulation of this is given in the associated CP.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate request/application

Regulation of this is given in the associated CP.

4.2 Certificate application processing

Regulation of this is given in the associated CP.

4.3 Certificate issuance

Regulation of this is given in the associated CP.

4.4 Certificate acceptance

Regulation of this is given in the associated CP.

4.5 Key pair and certificate usage

Regulation of this is given in the associated CP.

4.6 Certificate renewal

Not applicable. No renewal is allowed.

4.7 Certificate re-key

Regulation of this is given in the associated CP.

4.8 Certificate modification

Modification of certificate is not allowed.

4.9 Certificate revocation and suspension

Regulation of this is given in the associated CP.

4.10 Certificate status services

Not applicable. Self-signed certificate.

4.11 End of relationship with a sub CA

Regulation of this is given in the associated CP.

4.12 Key escrow and recovery

Not applicable.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1 Physical Security Controls

The NGRTS Information Security Policy (ISP) describes the procedures implemented in terms of security management. This policy and the associated procedures will not be published but is made available during (internal and external) audits and validation of conformance.

NGRTS Infrastructure are hosted in a private space under the sole control of NG Technologies hosted in a datacenter certified Tier 4. The datacenter guarantees contractually: physical access controls based on authorizations provided by NG Technologies, redundancy of power supply, air conditioning and Internet connection.

The datacenter guarantees, as well, fire prevention and protection against exposure to water damage.

5.1.1 Site location

The technical systems of NGRTS are in a datacenter certified Tier 4. All NGRTS systems are located in a private secure room inside an IT secured area in the datacenter.

All IT systems related to the operation, usage and maintenance of the Root CA is hosted in a physically offline perimeter. The access of this perimeter is strictly limited to authorized persons. The presence of at least the CISO or the CTO is mandatory for any access to this offline location. Any operation on the HSM operating the Root CA requires the physical presence of 3 persons among 5 secret bearers.

Even when a system administrator or a technical operator is authorized to access an NGRTS system, the provided credential and authorization does not allow him to access the system and location hosting the Root CA.

5.1.2 Physical access

Regulation of this is given in the associated CP.

5.1.3 Power supply and air conditioning

See 5.1 above.

5.1.4 Exposure to water damage

See 5.1 above.

5.1.5 Fire prevention and protection

See 5.1 above.

5.1.6 Storage of data carriers

Further details are in the associated CP.

5.1.7 Waste disposal

Further details are in the associated CP.

5.1.8 Offsite backup

Further details are in the associated CP.

5.2 Procedural controls

5.2.1 Trusted roles

A specific committee in NG Technologies is responsible of operational management of NG Technologies Remote Trust Services. This committee is called the “PKI Committee” (PKICOM or COMPKI) and is composed of NG Technologies employees and employees of subcontractors.

PKICOM is composed of people performing security roles as well as operational roles (registration, secret bearer, etc.).

PKICOM is composed of key individuals responsible for the security, operation and maintenance of NGRTS components.

The CA equipment and the associated PKI software are deactivated outside of the key ceremonies for which different types of participants may be involved depending on the operations carried out:

- Ceremony administrator (technical manager);
- Ceremony master;
- At least one external auditor;
- At least one external witness;
- At least one internal witness;
- Secret bearers;

Their respective tasks are specified in the key ceremony scripts.

Each intervention gives rise to a report indicating the operations carried out and the associated roles.

5.2.1.1 Security roles

The roles below include the mandatory trust roles listed in ETSI EN 319 411-01 (paragraph 6.4.4, OVR-6.4.4-02).

The roles approved by PKICOM are listed below. The role terminology of EN 319 401 is used.

Corresponding Trusted Role as defined in EN 319 401	Description
Chief Information Security Officer (CISO)	Responsible for all aspects related to the logical and physical security of the hardware infrastructure of the PKI.
System administrator/operator (SO)	Agents involved in the management and maintenance IT administration of the various components of the PKI.
System Auditor (SA)	Responsible of the planning and execution of internal audit functions.

In addition to the roles above, PKICOM includes the key role represented by Chief Technical Officer (CTO). He oversees the design, architecture, and the development of the technical components of the CA as well as the daily operating operations of the CA (updates, backups, restoration, etc.).

5.2.1.2 Operational roles

In addition to the roles above, additional roles are defined. The roles below can be assigned to employees without any security role.

Role	Description
Secret Bearer (SB)	Ensures the confidentiality, integrity, and availability of the sharing of secrets entrusted to him.

5.2.1.3 Assignment

The above roles are assigned only to:

- NG Technologies employees who provided all the administrative documents including Bulletin N ° 3 (or equivalent, for foreigners);
- Employees of an external supplier with a contract including confidentiality clauses. The contract must explicitly require full compliance with all security and operating policies of NG Technologies, including the IT charter and PDP (Personal Data Protection) policies.

5.2.2 Number of persons required per task

The following table specifies security-level tasks and assigns them to the proper role. Some roles are associated to an automatic (technical) function of NGRTS (no manual intervention).

Task	Role	Dual Control Principle	Comments
Verification of documents	PO		

Any operation on the cryptographic keys for the CA (generation, revocation, …)	CISO, CTO	Requires the physical presence of at least 3 SB among 6.	After authorization from the CEO and under the supervision of the SIC (Security Information Committee). The physical presence of the CTO or CISO is mandatory. Can only be done with the presence of auditors and witness (external and internal) based on key ceremony script.
Certification; initiation of processes for issuance of revocation lists	NGRTS		The operation is automatic with preconfigured frequency. The CTO or CISO can, however, force the issuance of a new CRL before the next update date.
Publication of certificates and revocationlists	NGRTS		
Knowledge of boot and administrator passwords	CISO, CTO		
Initiation and termination of processes(e.g. webserver, backup)	SO		After authorization from the CISO and under the supervision of the CISO or CTO.
Data backup	SO		After authorization from the CISO and under the supervision of the CISO or CTO.
Physical administration/maintenance or replacement of critical hardware (HSM)	CISO, CTO	Requires the physical presence of at least 3 SB among 6.	

Physical administration/maintenance or replacement of other systems	SO		After authorization from the CISO and under the supervision of the CISO or CTO.
Transfer of secrets from an SB to another.	CISO, CTO	Requires the physical presence of at least 3 SB among 6.	Based on key ceremony script.
Restoration of backup data for critical systems (HSM)	CISO, CTO	Requires the physical presence of at least 3 SB among 6.	Based on key ceremony script.
Internal review of procedures	CISO, SA		At regular intervals.
Audit	SA (internal and external)		
Issuance of physical authorizations	CISO, CTO		The approval of the CEO is required.
Review of implementation of secure development rules	CTO		

5.2.3 Identification and authentication for each role

Regulation of this is given in the associated CP.

5.2.4 Roles requiring segregation of duties

The following table shows roles requiring separation of duties.

Roles	Incompatible with
CISO	CTO
SO	SA
SA	SO
CTO	CISO
SB	

5.3 Safety measures for personnel

5.3.1 Qualifications, skills and authorizations required

Regulation of this is given in the associated CP.

5.3.2 Background check procedures

This is part of our internal recruitment procedure. Regulation of this is given in the associated CP.

5.3.3 Initial training requirements

An internal training period precedes any access to any software or hardware component of NGRTS.
CISO and CTO are responsible for preparing annually a training plan.

5.3.4 Continuing education requirements and frequency

See above. Further details are in the associated CP.

5.3.5 Frequency and sequence of rotation between different assignments

Not applicable.

5.3.6 Sanctions for unauthorized actions

Regulation of this is given in the associated CP.

5.3.7 Requirements for the staff of external service providers

Regulation of this is given in the associated CP.

5.3.8 Documentation provided to staff

Regulation of this is given in the associated CP.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Regulation of this is given in the associated CP.

5.4.2 Processing frequency of event logs

Regulation of this is given in the associated CP.

5.4.3 Retention period for event logs

Regulation of this is given in the associated CP.

5.4.4 Protection of event logs

Regulation of this is given in the associated CP.

5.4.5 How to Back Up Event Logs

Regulation of this is given in the associated CP.

5.4.6 Event log collection system

Regulation of this is given in the associated CP.

5.4.7 Notification of the recording of an event to the event manager

Regulation of this is given in the associated CP.

5.4.8 Vulnerability assessment

Regulation of this is given in the associated CP.

5.5 Data archiving

5.5.1 Types of data to archive

Regulation of this is given in the associated CP.

5.5.2 Archives retention period

Regulation of this is given in the associated CP.

5.5.3 Protection of archives

Regulation of this is given in the associated CP.

5.5.4 Archive backup procedure

Regulation of this is given in the associated CP.

5.5.5 Data timestamp requirements

Regulation of this is given in the associated CP.

5.5.6 Archives collection system

Regulation of this is given in the associated CP.

5.5.7 Archive recovery and verification procedures

Regulation of this is given in the associated CP.

5.6 Change of CA keys

Regulation of this is given in the associated CP.

5.7 Recovery following compromise and disaster

5.7.1 Reporting and handling procedures for incidents and compromises

Further details for of this are given in the associated CP.

NG Technologies implements incident and vulnerability management procedures. These procedures, under the supervision of CISO and the CTO, define NG Technologies procedures for incident detection, resolution, and communications. These documents are not public and are regularly checked by external and internal auditor.

A public email address is shared for incidents/Vulnerability notifications: security@ng-sign.com This email is shared internally and externally with all relying parties.

For any incident, the incident response team, decides whether to convene the Crisis Management Committee depending on the level of impact of the incident. Incident Response Team is composed from the following roles:

- CISO
- CTO
- R&D Engineers.

Crisis Management Committee role is taken by the Information Security Committee composed of:

- CEO
- CISO
- CTO

5.7.2 Recovery procedures in the event of corruption of IT resources (hardware, software and / or data)

Further details are given in the associated CP.
See 5.7.4 below.

5.7.3 Recovery procedures in the event of a compromise of the private key of a component

CA Key compromise is considered as the most critical incident according to NG Technologies Incident Management Procedure, with Level of Impact set to "Severe" and Urgency rated to "Very High". The following procedure is immediately launched once the compromise is detected:

- The exact scope of the incident is identified:
    - Total compromise: the private key has been leaked outside the secure environment.
    - Undetermined compromise: the private key has not been leaked, but an undetermined set of objects (certificates, CRLs…) have been signed without authorization.
    - Determined compromise: the private key has not been leaked and a determined and identified object has been signed without authorization.
- The first report is presented to the Crisis Management Committee (see above) which decides the next actions.
- Relying parties and NGRTS users are notified. The notification may be sent to only a subset of relying parties and users.
- In all cases, the national regulation authority is immediately informed, and the initial report is shared.
- Depending on the compromise type, the Crisis Management Committee may decide to immediately revoke the CA and all certificates signed by this CA.
- If necessary, the Crisis Management Committee may decide to immediately turn off the CA systems to avoid any incorrect/malicious publication of a compromised object.
- Once the incident is under control, NG Technologies undertakes to publish an incident report. The report may be published at once after the resolution of the incident or may be in a form of a series of updates according to the progress of the implementation of the response.

5.7.4 Capacities for business continuity following a disaster

The capacity for business continuity following a disaster is addressed by the "Business Continuity Plan". Following a disaster, NG Technologies sets up the appropriate actions to restore the affected services. NG Technologies is using an architecture redundant for its critical services.

This CP does not allow the issuance of intermediate CA certificates for other entities other than NG Technologies. The "Business Continuity Plan" is managed to handle only these certificates.

In case of an extremely major disaster, the revocation service the ability to revoke an intermediate CA) is designed to be restored in less than 5 days.

Upon resumption of activity, the CA implements all the necessary measures to prevent a similar accident from happening again. Restoration operations are carried out by personnel occupying Trusted Roles. The Disaster Recovery Plan is tested regularly.

5.8 End of life of the CA

5.8.1 Activity transfer

Transfer is not allowed.

5.8.2 Cessation of activity

Regulation of this is given in the associated CP.

6 TECHNICAL SECURITY MEASURES

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

6.1.1.1 CA Keys

Regulation of this is given in the associated CP.

6.1.2 Transmission of the private key of a daughter CA

Not applicable.

6.1.3 Transmission of the public key of a daughter CA

Regulation of this is given in the associated CP.

6.1.4 Transmission of the CA's public key to users

Regulation of this is given in the associated CP.

6.1.5 Key sizes

Regulation of this is given in the associated CP.

6.1.6 Checking the generation of key pair parameters and their quality

Regulation of this is given in the associated CP.

6.1.7 Objectives of the use of the key

Regulation of this is given in the associated CP.

6.2 Security measures for the protection of private keys and for cryptographic modules

6.2.1 Standards and security measures for cryptographic modules

Regulation of this is given in the associated CP.

6.2.2 Control of the private key by several people

The CA's private key is controlled by activation data stored on smart cards given to secret bearers during the key ceremony.

The following rules apply:

- Physical or logical access to the environments including an HSM device is limited to persons belonging to the COMPKI;
- Any access must be authorized by the CISO or his replacement and must be conformant to the approved accreditation matrix;
- Carrying out an operation with a key protected by HSM requires authentication based on the physical presence of a quorum of people (designated m = 3 out of n = 6);
- Part of the "secrecy" allowing the operation to be carried out is entrusted to each member of the quorum on a smart card;
- Secrets allowing an operation to be carried out on an HSM device should only be entrusted to a person having the role of "secret bearer";
- Each card is protected by a personal password known only by the secret bearer;
- Each secret bearer has a secure individual safe;
- Smart card safes must be placed on at least 2 sites so as to allow cards from each site to reach a quorum.

Each secret bearer has a secure personal safe protected by a key and a digital code that is known only to him.

6.2.3 Escrow of the private key

NGRTS does not authorize the escrow of the private keys of the CA or the private keys of the Holders.

6.2.4 Backup copy of the private key

Regulation of this is given in the associated CP.

6.2.5 Archiving the private key

No archiving is done for private keys.

6.2.6 Transfer of the private key to / from the cryptographic module

Regulation of this is given in the associated CP.

6.2.7 Storage of the private key in a cryptographic module

Regulation of this is given in the associated CP.

6.2.8 Private key activation method

6.2.8.1 CA private key

The activation of the CA's private key requires the presence of two secret bearers having trusted roles and possessing the activation data (smart card and a pin code).

Activation takes place during a key ceremony. A ceremony report is established at the end of the ceremony.

The ceremony script, the minutes and the attendance list are archived at the end of the ceremony (see section 5.5).

The rules listed in 6.2.2 apply.

6.2.8.2 Holders' private key

See **Error! Reference source not found.** and the associated CP for further details.

6.2.9 Private key deactivation method

Regulation of this is given in the associated CP.

6.2.10 Method of destroying private keys

Regulation of this is given in the associated CP.

6.2.11 Qualification level of the cryptographic module and the private key protection devices

Regulation of this is given in the associated CP.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

Regulation of this is given in the associated CP.

6.3.2 Lifespans of key pairs and Certificates

Regulation of this is given in the associated CP.

6.4 Activation Data

Regulation of this is given in the associated CP.

6.5 IT systems security measures

6.5.1 Technical security measures specific to IT systems

Regulation of this is given in the associated CP.

6.5.2 IT systems qualification level

Not applicable.

6.6 System security measures during their lifecycle

6.6.1 Security measures related to systems development

Regulation of this is given in the associated CP.

6.6.2 Safety management measures

Regulation of this is given in the associated CP.

6.6.3 Systems lifecycle security assessment level

Regulation of this is given in the associated CP.

6.7 Network security measures

Regulation of this is given in the associated CP.

6.8 Timestamp / Dating system

Regulation of this is given in the associated CP.

7 PROFILE OF CERTIFICATES, OCSPS AND CRLS

7.1 Certificate Profile

7.1.1 Certificate of the Intermediate Certification Authority RT CA

Regulation of this is given in the associated CP.

7.1.2 Holders Certificates

Regulation of this is given in the associated CP.

7.2 CRL Profile

Regulation of this is given in the associated CP.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequencies and / or circumstances of evaluations

Regulation of this is given in the associated CP.

8.2 Identities / qualifications of assessors

Regulation of this is given in the associated CP.

8.3 Relations between evaluators and evaluated entities

Regulation of this is given in the associated CP.

8.4 Topics covered by the reviews

Regulation of this is given in the associated CP.

8.5 Actions taken following the conclusions of the evaluations

Regulation of this is given in the associated CP.

8.6 Communication of results

Regulation of this is given in the associated CP.

9 OTHER COMMERCIAL AND LEGAL ISSUES

Regulation of this is given in the associated CP.