NG Technologies Remote Trust Services

Certification Policy of NG Technologies Root Certification Authority

Identifier	PKI-CP-ROOT-CA
Version	1.0
Description	NG Technologies Root CA Certification Policy.
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

INDEX

Acronyms

- **CA:** Certification Authority (AC in French)
- **CP:** Certification Policy
- **RA:** Registration Authority (AR in French)
- **ANCE:** National Certification Agency
- **CISO:** Chief Information Security Officer
- **CGU:** General conditions of use
- **CSR:** Certificate Signature Request
- **DPC:** Certification Practices Statements
- **ISC:** Information Security Committee
- **INPDP:** National body for the protection of personal data
- **LCR:** List of revoked certificates
- **LAR:** List of Revoked Authority certificates
- **LCR:** List of Revoked User Certificates
- **OTP:** One Time Password
- **OCSP:** Online Certificate Service Protocol
- **PKI:** Public Key Infrastructure
- **PSI:** Information Security Policy
- **RSI:** Information System Manager
- **RSSI:** Information System Security Manager
- **SSCD**: Secure Signature Creation Device
- **TSP:** Timestamp Protocol

1 INTRODUCTION

1.1 General presentation

This document constitutes the Certification Policy 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.

1.2 Document identification

This CP is identified by the OID **2.16.788.2.1.1.**

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) 1}) has been registered for NG Technologies services [1]at Instance Nationale des Télécommunications (INT) as the organization representing Tunisia at the ITU.

The certification policies of the Sub CAs of this root Certification Authority will be incrementally assigned an OID 2.16.788.2.1.x.

The Certification Policy and Certification Practice Statement are hereinafter referred to as "PC" and "CPS".

1.3 Components of Key Management Infrastructure (KMI)

1.3.1 Overview

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 and designed by the unit NG PKI. NG PKI is composed of this Root Certification Authority and one or more intermediate (sub) Certification Authorities.

1.3.2 Root CA perimeters

Root CA is made up of several functional blocks, in particular the functions of CA and RA.

1.3.3 CA functions

The CA provides certificate management services for the attached sub CAs:

- Processing of certificate requests;
- Issuance of certificates to applicants;
- Processing revocation requests;
- Publication of its certificate and LARs.

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

The root CA signs the certificates and LARs that it issues with its private key and is responsible for them.

These features are provided by PKI software used in conjunction with an HSM for generation, private key encryption, and signing of certificates and LARs.

1.3.3.1 Certificate generation function

This function generates the certificates from the information transmitted by the PKI software in the form of a CSR and a certificate template defined during the configuration of the root CA. This function can only be done in the context of a key ceremony and in the presence of internal and external witnesses (notary and auditor).

1.3.3.2 Function for generating the secret elements of a daughter CA

Not applicable. The keys of a sub CA are generated at its level.

1.3.3.3 Publication function

The Root CA system is offline. However, the Root CA certificate can be exported to an external storage device.

It can then be published on a public server to be used for validating certificate chains.

1.3.3.4 Revocation management function

This function processes revocation requests that are submitted to the CA. This results in the immediate publication of a new LAR. This LAR can be exported to an external storage device.

1.3.4 RA function

No Registration Authority associated with this CA. This Authority only signs sub CAs under the control of a key ceremony in the presence of internal and external witnesses (notary and auditor).

The PKI software installed with the CA allows, through an administration tool, to submit a CSR and to retrieve the corresponding certificate.

1.4 Use of certificates

1.4.1 Applicable areas of use

The key pair of this CA is only used to sign sub CAs and their LARs issued at regular intervals.

1.4.2 Areas of use prohibited

All other usage is forbidden.

1.5 Policy management

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.

The authorized contact for any remark, request for additional information, complaint or submission of a dispute file concerning this CP is:

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

2 RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION TO BE PUBLISHED

2.1 Entities responsible for making information available

NG Technologies is in charge of the publication of this PC.

NG Technologies is also in charge of the administration and execution of operations of generation and publication of LARs.

2.2 Information to be published

The information published is:

- This CP and the associated CPS: published on the NG Technologies website with free access and link from the home page of the site;
- The LARs issued by the Root CA are also published on a dedicated page on the NG Technologies website with free access and link from the home page.
- The public certificate of the certification authority in PEM and DER formats.

2.3 Publication deadlines and frequencies

The Certification Policy is published after internal validation within the PKI Committee and final approval of the CEO.

LARs are published within 60 minutes of their generation.

2.4 Access control to published information

The PC and the LARs are freely accessible and read only from the NG Technologies website without any restriction.

The published elements are signed electronically in order to be duly authenticated.

Access to modify information is strictly limited to authorized internal administration functions which have write rights to the shared environment for depositing this information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The names used conform to the specifications of the X.500 standard.

The "issuer" and "subject" fields of certificates are identified by an X.500-type "Distinguished Name" (DN) in the form of a "PrintableString".

3.1.2 Pseudonymization

Not applicable.

3.1.3 Rules for interpreting the different forms of name

Not applicable.

3.1.4 Uniqueness of names

The “Common Name” (CN) field is unique for each sub CA. Throughout the life of the CA, a CN allocated to a sub CA cannot therefore be allocated to another CA.

3.1.5 Identification, authentication and role of trademarks

Not applicable.

3.2 Initial identity validation

3.2.1 Method to prove possession of the private key

The signing of a CSR by the associated private key provides this guarantee in combination with the PV of the key ceremony for the generation of the key pair of the daughter CA. Key Ceremony PV is considered public and is published.

This is the only way allowed by the PKI software to submit a certificate request.

3.2.2 Validation of the identity of an organization

The naming data of a sub CA to be signed are communicated for validation in the preparation phase of the key ceremony.

Only sub CA managed by NG Technologies are allowed.

3.2.3 Validation of an individual's identity

Not applicable.

3.2.4 Unverified information

The information in the certificate is validated during the preparation phase of the key ceremony.

3.2.5 Validation of the authority of the applicant

Only a sub CA affiliated with NG Technologies can be issued by the Root CA.

3.2.6 AC cross certification

Not applicable.

3.3 Identification and validation of a key renewal request

3.3.1 Identification and validation for a current renewal

The identification and validation for a current renewal of a sub CA certificate is carried out in accordance with section 3.2.

3.3.2 Identification and validation for renewal after revocation

The identification and validation for a renewal following revocation of a child CA certificate are carried out in accordance with section 3.2.

3.4 Identification and validation of a revocation request

The revocation of a sub CA can only be decided by NG Technologies. No external parameters are used. The revocation must be justified.

4 OPERATIONAL REQUIREMENTS FOR THE CERTIFICATE LIFECYCLE

4.1 Certificate request

4.1.1 Origin of a certificate request

The only possible origin for a certificate request is an internal request of NG Technologies.

4.1.2 Process and responsibilities for issuing a certificate request

NG Technologies is the sole entity responsible for establishing a certificate request.

4.2 Processing a certificate request

4.2.1 Execution of the request identification and validation process

The identification and validation of the request are processed during the preparation phase of the key ceremony.

4.2.2 Acceptance or rejection of the request

Not applicable.

4.2.3 Duration of the certificate

Not applicable.

4.3 Issuance of the certificate

4.3.1 CA actions regarding the issuance of the certificate

This operation requires the reactivation of the Root CA and involves the presence of at least three bearers of secrets as well as the bearers of the roles necessary for the realization of the key ceremony. Roles must include at least one internal witness and at least one external witness.

After its validation, the CSR is submitted to the Root CA through a script during a key ceremony.

The naming elements are displayed and compared to the values given in the key ceremony script. If they are consistent, a certificate template is chosen and the request is submitted to the CA which provides the certificate in return, otherwise the request is rejected.

The certificate is copied into removable media to be published manually after the session.

4.3.2 Notification by the CA of the issuance of the bearer certificate

The certificate is issued after the key ceremony by exporting the certificate to removable media.

4.4 Acceptance of the certificate

4.4.1 Procedure for accepting the certificate

Acceptance is tacit.

4.4.2 Publication of the certificate

The certificate is exported from the Root CA environment to removable media. Then it is published as quickly as possible as shown in the section0.

4.4.3 Notification by the CA to the other entities of the issuance of the certificate

Not applicable.

4.5 Use of the key pair and the certificate

4.5.1 Use of the private key and certificate

The use of the private key of a sub CA and of the associated certificate is strictly limited to the signing of certificates and CRLs within this CA according to the intended use in its PC.

Technically, this use is also indicated via the “Key_Usage” extension of its certificate.

4.5.2 Use of the public key and the certificate by third parties

Not applicable.

4.6 Renewal of a certificate

Renewal without key change is not allowed.

4.7 Issuance of a new certificate following a change of the key pair

This section deals with the issuance of a new certificate to a sub CA linked to the generation of a new key pair.

4.7.1 Possible causes of changing a key pair

The main cause for renewal is expiration. Early renewals are also possible, for example for reasons of technical maintainability or the weakness of a key or an algorithm used in the current certificate.

4.7.2 Origin of a request for a new certificate

The origin is the same as for an initial request. See section 4.1.1.

4.7.3 Procedure for processing a request for a new certificate

The procedure is the same as for an initial request. See section 4.2.

4.7.4 Notification to the bearer of the establishment of the new certificate

The procedure is the same as for an initial request. See section 4.3.2.

4.7.5 Procedure for accepting the new certificate

The procedure is the same as for an initial request. See section4.1.1.

4.7.6 Publication of the new certificate

The procedure is the same as for an initial request. See section4.4.2.

4.7.7 Notification by the CA to the other entities of the issuance of the new certificate

The procedure is the same as for an initial request. See section 4.4.3.

4.8 Modification of the certificate

Modification of certificate is not allowed in this CP.

4.9 Revocation and suspension of certificates

4.9.1 Possible causes of revocation

4.9.1.1 Certificate of a sub CA

The possible causes of revocation of a sub CA issued by the CA subject of this PC are numerous, for example:

- An error detected in the content of the certificate that appeared after the key ceremony;
- Cessation of activity;
- A suspicion of compromise, a compromise, the loss or the theft of his private key;
- Regulatory developments on the algorithms used.

4.9.1.2 CA certificate subject to this CP

There are also many possible reasons for revocation, in particular:

- Cessation of activity;
- A suspicion of compromise, a compromise, the loss or the theft of his private key;

In this case, all the sub Certification Authorities must first be revoked and a last LAR published before the final shutdown.

4.9.2 Origin of a revocation request

This type of revocation can only be requested after consultation by the PKI committee of NG Technologies and following the drafting of a technical report justifying the request.

4.9.3 Procedure for processing a revocation request

This operation requires the reactivation of the Root CA and involves the physical presence of several trusted roles. A person must be designated in advance as the master of the revocation session.

The revocation is carried out during a key ceremony on the root CA via a technical tool of the PKI solution. This results in the immediate creation of a new LAR which can be exported to removable media.

The session supervisor must ensure communication of the LAR to the technical service responsible for its publication. He must also produce a meeting report.

If the revocation concerns the root, all the sub CAs must first be revoked.

4.9.4 Deadline for formulating the revocation request

The request is considered as soon as the decision is made.

4.9.5 Processing time by the root CA of a revocation request

This operation requires the reactivation of the root CA. It is done based a key ceremony script with the physical presence of several roles.

It must be planned within 72 working hours after the decision has been taken.

4.9.6 Revocation checking requirements by certificate users

The LAR is made available in the form of a file to third-party applications which perform this verification.

4.9.7 Frequency of establishment of LARs

LARs are generated upon each revocation or by default every 12 months. However, a new LAR can be systematically published following a revocation of a intermediate CA.

4.9.8 Maximum time limit for publication of a LAR

A LAR is published within a maximum period of 8 hours following its generation.

4.9.9 Availability of an online certificate revocation and status verification system

Service not offered.

4.9.10 Requirements for online certificate revocation checking by certificate users

Not applicable.

4.9.11 Other available means of information on revocations

Not applicable.

4.9.12 Specific requirements in case of compromise of the private key

The revocation procedure must be triggered immediately upon detection of a compromise. See section 4.9.

4.9.13 Possible causes of a suspension

Suspension is not permitted. No manipulation on the PKI software allows this to be done.

4.9.14 Origin of a suspension request

Not applicable.

4.9.15 Procedure for processing a suspension request

Not applicable.

4.9.16 Limits of the suspension period of a CA

Not applicable.

4.10 Certificate status information function

Not applicable. Self-signed certificate.

4.11 End of relationship with a sub CA

In the event of termination of the relationship, for whatever reason, the CA's certificate must be revoked.

4.12 Key escrow and recovery

There is no escrow of a sub CA key at the root CA level.

5 NON- TECHNICAL SECURITY MEASURES

5.1 Physical security measures

This CA is hosted in a data center offering the necessary guarantees in terms of access control, fire safety, backups, etc.

The CA server, its HSM and the associated PKI software are installed in premises whose access is controlled and reserved for authorized personnel designated by NG Technologies. This assembly forming the technical environment of the CA is installed without any network connection (offline) and physically independent of any other service operated by NG Technologies.

The initialization and activation of the AC implies the presence of several complementary trust roles between them.

5.2 Procedural security measures

5.2.1 Trust roles

The functions operated on the Root CA are distributed over several trust roles in order to ensure the separation of knowledge for sensitive tasks. Each stakeholder has an identification factor linked to a given role of trust.

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.

5.2.2 Number of people required per task

Depending on the type of operations performed, the number and type of roles and people to be present are different. The need is greatest for the creation of the CA with the phases of configuring servers and HSMs and PKI software installations that also involve system administrators.

5.2.3 Identification and authentication for each role

The identification of each person is done on three levels:

- Access to the data center which hosts the CA requires the presentation of an identity document to verify that the worker is on the list of persons authorized to access the space allocated to the PKI NG Technologies;
- Access to the space allocated to the NG Technologies PKI requires a double identification to verify that the user is authorized to act on the NG Technologies PKI system;
- Access to the CA equipment and the associated PKI software requires a second authentication to verify that the participant is authorized to access this CA.

5.2.4 Roles requiring separation of responsibilities

Several roles can be assigned to the same person when the combination does not compromise the security of the functions implemented.

5.3 Safety measures for personnel

5.3.1 Qualifications, skills and authorizations required

Staff operating in trusted roles within the PKI are informed of their relative responsibilities (commitment document, DPC document) as well as the procedures related to system security and internal regulations, with which they must comply.

The supervisory staff are trained and sensitized in security and risk management to fully assume their responsibilities vis-à-vis the PKI.

5.3.2 Background check procedures

In particular, staff members must not have a court conviction or be in a situation of conflict of interest in contradiction with their duties. They give their employer a copy of bulletin n ° 3 of their criminal record for Tunisians or equivalent for foreigners as part of the hiring procedure as well as when submitting their liability commitment.

The candidate's application file is submitted for validation to the Management.

The criminal record check is renewed in a regular basis.

The staff members responsible for operating the Certification services are not responsible for the commercial aspects related to these services and are free from any conflict of interest which could influence the way of carrying out the operations for which they are responsible. In this regard, they undertake to confirm in writing, when accepting the role of trust within the PKI, the absence of any conflict of interest linked to the exercise of this new activity.

5.3.3 Initial training requirements

IT Staff are trained in CA software, hardware and operating procedures.

Staff were made aware of the implications of the operations for which they are responsible through safety awareness.

5.3.4 Continuing education requirements and frequency

The personnel concerned receive adequate information and training according to the responsibilities entrusted.

5.3.5 Frequency and sequence of rotation between different assignments

Not applicable.

5.3.6 Sanctions for unauthorized actions

Each person assuming a role in the management of the PKI must sign a commitment of responsibilities. This commitment clearly explains the role of the person and the associated internal regulations. The regulations provide for appropriate administrative disciplinary sanctions in the event of misconduct.

5.3.7 Requirements for the staff of external service providers

The requirements vis-à-vis external service providers must be contractualized. The requirements of paragraph 5.3 are applicable to external providers. These requirements are explained in the contracts with the service providers.

5.3.8 Documentation provided to staff

Each person has at least the documentation relating to the operational procedures and specific tools that he implements, as well as the general policies and practices of the component within which he works.

5.4 Audit data compilation procedures

All the administration operations concerning the CA are plotted with:

- Archived logs generated by the PKI software and exported to an external storage device;
- Ceremonies documents (papers) and scripts.

5.4.1 Type of events to record

The event logs explicitly include the identifier of the executor (software or operator) of the operation, the date, the type of operation and a description.

5.4.1.1 Computer traces of the CA

Each component of the CA PKI software logs events and incidents concerning it. Below is a non-exhaustive list:

- Start-up and shutdown of computer systems and applications;
- Creation of the key pair and signature of CSR;
- Creation of certificates;
- Revocation of certificates;
- Publication of LARs.

5.4.1.2 *Access control*

Access to the data center keeps a log of accesses with the identity of the person and the purpose of their access request.

Access to the space reserved for the CA is also logged.

5.4.1.3 *Handwritten traces*

Manual journals concern:

- Key ceremonies and their PV;
- LAR's creations;
- The revocation or renewal of a CA;
- Interventions requiring access to sensitive premises and safes, for example:
    - Restoring the HSM to service or restoring from backups following a failure;
    - Scrapping.

5.4.2 Processing frequency of event logs

AC logs are archived. Archival and export of the logs are part of the key ceremony.

5.4.3 Retention period for event logs

Logs are retained for the life of the CA.

5.4.4 Protection of event logs

Both computer and manuscript journals are protected by strict access control limited to authorized persons only.

5.4.5 How to Back Up Event Logs

CA logs are automatically archived. Note that the AC software is off outside of key ceremonies. No event log is therefore generated outside of a ceremony. Logs are exported in two copies stored into two sites.

5.4.6 Event log collection system

The main copy of logs is archived in the same offline environment of the CA.

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

Events are recorded automatically without intervention.

5.4.8 Vulnerability assessment

As the CA is deactivated outside of key ceremonies, there is no systematic and regular analysis of the logs. This is only done when there is a need for internal investigation.

5.5 Data archiving

5.5.1 Types of data to archive

Archiving concerns both handwritten documents (e.g PVs) and electronic documents (e.g documentation, PC, PVs, journals).

The archiving must record the following operations:

- Sub CA certificate requests;
- Renewal requests;
- Revocation requests.

Electronic documents (PC, PVs, etc.) are archived with version management.

Documents / data to be archived include:

- CP / CPS;
- Files of creation and revocation requests;
- The certificates of the sub CA issued as well as the associated LARs;
- Technical logs of all components;
- The documentary repository (procedures, policies, technical architectures, access requests, forms…).

5.5.2 Archives retention period

20 years after the life of the AC.

5.5.3 Protection of archives

The paper archives will be kept physically in a dedicated space. One version is digitized for electronic archiving.

5.5.4 Archive backup procedure

See section 5.5.3

5.5.5 Data time stamping requirements

The root CA server clock is synchronized to a reliable external source.

5.5.5 Archives collection system

Collection is organized after each operation on the CA.

5.5.6 Retrieval and verification of archives

The archives are saved in the same offline environment of the CA. They can be retrieved for investigation at any time. Recovery requires obtaining an authorization signed by the security manager or his substitute and the presence of several trusted roles.

5.6 Change of CA key

The CA cannot generate a child CA certificate with an end date after its certificate expiration date.

It must be renewed at the latest when it expires or before the deadline if, for example, it is necessary to move towards stronger algorithms, greater key lengths or if it is necessary to sign a daughter CA whose desired deadline is after the maturity of the root CA. In this case the old root CA is maintained in order to be able to revoke the CAs that it has signed and to continue to publish its LARs. The news is used to sign and revoke new CAs and publish their LARs.

5.7 Recovery following compromise and disaster

5.7.1 Reporting and handling procedures for incidents and compromises

Incident management is the responsibility of the security manager at NG technologies (CISO for Chief Information Security Officer). Incidents are reported to the ISC (Information Security Committee) as soon as they are detected. The committee will implement the appropriate actions according to the requirements of this CP and of NG Technologies Information Security Policy.

5.7.2 Recovery procedures in the event of corruption of IT resources

A sequence of actions is to be implemented depending on the incident. In the event of a hardware failure, the action can range from a reboot to the replacement of a given device, during the repair.

In the event of a software incident (bug), the security manager writes a bug report on our ticket system and immediately enters the development roadmap.

When it is relevant (inability to launch a revocation operation), the incident can lead to a decision being taken which impacts a sub CA (note that all the sub CAs of this CA are under the control of NG Technologies).

As it is an offline CA, it does not need to ensure a continuous operation process.

5.7.3 Recovery procedures in case of compromise of the private key

If the CA's private key is compromised or is suspected of being compromised, if it is destroyed or if the algorithm used is compromised:

- After investigating the event, NG Technologies can decide whether or not to revoke the Root CA certificate;
- If it is decided to revoke the relevant certificate from the Root CA:
  - All the certificates issued by the sub CAs and signed with their private key concerned are revoked, and the associated plan in the PCs of the sub CAs is triggered;
  - All certificates issued by the Root CA and signed with the affected private key are revoked.
- If an algorithm is compromised, then it is replaced;
- A new key pair is generated and a new corresponding Root CA certificate is issued;
- NG Technologies decides on the destination communication plan:
  - Communication of a report to the national regulation body (ANCE)
  - Subscribers and certificate users of the sub CAs (all of which are managed by NG Technologies)

5.7.4 Capacities for business continuity following a disaster

This AC does not need continuous operation, it is in fact deactivated most of the time. The backups in place allow the service to be rebuilt within a reasonable period of a few days.

5.8 End of life of the CA

5.8.1 Activity transfer

In the event of a decision of Activity Transfer, NG Technologies writes a full report including:

- The reasons for this decision;
- Detailed description of the CA (number of sub CA, certificates issued by each sub CA…);
- A summary of current charges to keep all systems functioning;
- The latest versions of the risk matrix, current actions and the latest audit reports.

NG Technologies undertakes to make the appropriate efforts to find a Certification Authority to succeed the NG Technologies Authority. If a successor is found who can assume all the responsibilities of the NG Technologies certification authority, a succession plan can be established. The succession plan may still include the obligation to execute the cession of activity plan of this certification authority or of one or more of sub CAs issued by this certification authority.

The transfer must be realized in conformance with current regulation. In particular, the successor must prove conformance to this regulation. The transfer plan covers the following aspects:

- The transfer intention and the report are communicated to the National Regulatory Authority at least 3 months before the transfer date;

- For each sub CA concerned with the transfer, all certificates holders are notified using the email address used with the certificate request. Each certificate holder:
    - is notified of the successor identity.
    - is informed that he can refuses the transfer by a simple reply to the notification email at most 1 month after the initial notification
    - is informed that in case of refusal, his certificate will be revoked;
- Notification emails are sent at least 3 months before the transfer and a second time 75 days before the transfer.
- In case a holder refuses the transfer, the sub CA must revoke the holder certificate.
- Notification of all customers and partners;

5.8.2 Cessation of activity

In the event of a permanent shutdown, the CA sets up an end-of-life plan. This end-of-life plan covers the following aspects:

- Notification of ANCE as the National Regulatory Authority. This notification must be made at least 3 months before the date scheduled for the actual revocation of the CA and the certificates issued.
- Notification of all customers and partners;
- Activation of the cessation of activity of all sub CAs issued by this Root CA (application of the measures provided for the cessation of activity plan in the certification policies of sub CAs);
- The revocation of the certificate of this CA;
- The destruction of his private key and associated secrets

6 TECHNICAL SECURITY MEASURES

6.1 Generation and installation of key pairs

6.1.1 Generation of root CA key pairs

The generation of CA key pairs is performed in an HSM whose qualification level is described in chapter 6.2.11 of this document.

This generation takes place during a key ceremony in the secure premises housing the CA systems. It involves different trust roles for the activation of the HSM and PKI software used.

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

It is transmitted in the form of a CSR in PKCS # 10 format which allows its integrity to be checked.

6.1.4 Transmission of the CA's public key to users

It is transmitted via its certificate during the signing ceremonies of the daughter CAs at the same time as the daughter certificate.

6.1.5 Key size

8192 bits or more for renewals.

6.1.6 Checking the generation of key pair parameters and their quality

The quality of the generation is checked upon receipt of the CSR by the Certification Authority. The key sizes must correspond to the template of the daughter CA concerned.

6.1.7 Objectives of the use of the key

The private keys of this AC and daughter ACs are limited to signing certificates and CRLs. This is surrounded by the KeyUsage extension with the values keyCertSign and CRLSign. This extension is critical.

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

6.2.1 Standards and security measures for cryptographic modules

The generation of CA key pairs is performed in an HSM whose qualification level is described in chapter 6.2.11 of this document.

6.2.2 Control of the private key by several people

The generation and activation of the CA's private key implement a system for sharing secrets between several trusted roles. These procedures are detailed in the key ceremony script.

6.2.3 Escrow of the private key

The private keys of the root CA or of the daughter CAs are not sequestered.

6.2.4 Private key backup

The private key of the root CA is saved through the procedures of the HSM builder.

The backup takes the form of a file containing a cryptogram of the private key encrypted by the master key of the HSM.

6.2.5 Archiving the private key

The private keys of the root CA and its child CAs are not archived.

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

This transfer is only possible via the procedures of the backup / restore manufacturer.

6.2.7 Storage of the private key in a cryptographic module

The private key is protected by an HSM evaluated as defined in chapter 6.2.11 or encrypted by the master key of the HSM in the event of external backup, in accordance with the manufacturer's backup procedures.

6.2.8 Private key activation method

The CA private key can only be activated during a key ceremony, in the presence of several trusted roles that hold activation data of the HSM and parts of its master key.

6.2.9 Private key deactivation method

It is deactivated by removing it from the HSM after backup as well as by uninstalling the software from the
HSM.

6.2.10 Method of destroying private keys

Destruction can be performed by an HSM administrator after activation. In addition, all backups must be destroyed either through secure deletion software or by physical destruction of the removable backup media.

6.2.11 Qualification level of the cryptographic module and authentication devices

FIPS 140-2 L3.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

The public keys of this CA and each daughter are archived electronically, and a copy is posted for the public on the website.

6.3.2 Lifespans of key pairs and certificates

The CA cannot issue a daughter CA certificate with a lifetime greater than its own. The lifespans of key pairs and certificates are defined within the certificates themselves.

- The lifespan of the CA Root CA certificate: 25 years
- The lifespan of intermediate CA certificates signed by this CA: 20 years
- The lifespan of Time Stamping Authority certificates: 5 years

6.4 Activation data

6.4.1 Generation and installation of activation data

The HSM activation data is generated during the CA initialization key ceremony.

6.4.2 Activation data protection

These data are the responsibility of the secret bearers who have safes to keep them in a secure environment.

6.4.3 Other aspects related to activation data

Not applicable.

6.5 IT systems security measures

6.5.1 Technical security requirements specific to IT systems

The AC management tool (NG PKI) meets the following security objectives:

- All operations are traced;
- Guarantee of integrity: the fingerprint (hash of the binary) is verified before any operation. This imprint is mentioned in the report of the operation;

6.5.2 IT systems qualification level

This CP does not formulate any specific requirement on the subject.

6.6 System security measures during their lifecycle

6.6.1 Security measures related to systems development

Not applicable.

6.6.2 Safety management measures

NG PKI software was developed following strict rules in terms of QA (unit tests and code quality).

6.6.3 Systems lifecycle security assessment level

Any release (evolution) is preceded by the realization of a matrix of tests in a test environment. The release history is archived with a Release Notes for each version.

6.7 Network security measures

The CA server is not connected to any network other than key ceremonial operations in which a private and closed network is specially set up.

6.8 Timestamp / Dating system

The server clock is synchronized to a reliable external source. Synchronization is only triggered when the PKI software is commissioned. Apart from the use of the PKI software, no synchronization is possible (offline and deactivated environment).

7 CERTIFICATE, OCSP AND CRL PROFILES

7.1 Certificate profile

The certificates issued by this CA contain the following basic fields:

- Version: version of the X.509 certificate (v3);
- Serial number: serial number of the certificate (unique value for each certificate issued);
- Signature: OID of the algorithm used by the CA to sign the certificate;
- Issuer: value of the DN (X.500) of the CA issuing the certificate;
- Validity: activation and expiration date of the certificate;
- Subject: DN (X.500) value of the equipment;
- Subject Public Key Info: OID of the algorithm and value of the public key of the equipment;
- Extensions: list of extensions.

To these fields are added extensions which can be critical or non-critical. These are a combination of extensions from the CSRs of the child CAs and extensions imposed by the certificate template at that CA.

7.1.1 NG Technologies Root CA Certificate

The CA certificate is defined below. It is presented in two parts: the basic fields and the extensions.

Basic fields:

Fields	Value
Version	2 (V3)
Serial Number	**821583767049472149835271317976805207825588061867**
Signature (OID compliant with RFC 5280)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = NG Technologies Root CA, O = NG Technologies, OU = NG PKI, C = TN
Validiy	25 years
Subject	CN = NG Technologies Root CA, O = NG Technologies, OU = NG PKI, C = TN
Subject Public Key Info	RSA 8192 bits

Extensions:

Fields	Criticality	value
Authority Key Identifier	No	4DF2C7882770E188BD099317D8E13D2785C72403
Subject Key Identifier	No	4DF2C7882770E188BD099317D8E13D2785C72403

Key Usage	Yes	keyCertSign, CRLSign
Basic Constraint	Yes	• Certificate Authority: yes • Maximum Path Length: Unlimited

7.1.2 Sub CA Certificates

The template of a Sub CA (child CA) must be described in its own Certification Policy. It must comply with all the technical constraints defined in this Certification Policy.

7.2 LAR Profile

The LARs issued include the following fields:

- Version: version of the CRL standard (v2 - RFC 5280);
- Signature: OID of the algorithm used by the CA to sign the LAR;
- Issuer: value of the DN (X.500) of the CA issuing the LAR;
- This Update: date of generation of this update of the LAR;
- Next Update: date of generation of the next update of the LAR;
- Revoked Certificates: list of revoked certificates with their serial number, date of revocation and reason;
- CRL Extensions: list of extensions.

The template used is defined below. It is presented in two parts: the basic fields and the extensions.

Basic fields:

Fields	Value
Version	1 (V2)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN=NG Technologies Root CA, O=NG Technologies, OU=NG PKI, C=TN
ThisUpdate	Date of issue
NextUpdate	Issue date + 12 months
Revoked Certificates	List of revoked CA certificates

Extensions:

Fields	Criticality	value
Authority Key Identifier	No	Issuer DN: CN=NG Technologies Root CA, O=NG Technologies, OU=NG PKI,C=TN Issuer serial number: 821583767049472149835271317976805207825588061867
CRL Number	No	LAR number

7.3 OCSP Profile

The root CA does not implement an OCSP service.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequencies and / or circumstances of evaluations

NGRTS PKI is audited at least once a year for regulatory security audits and at least once every 2 years for ETSI EN 319 411 compliance audits.

8.2 Identities / qualifications of assessors

Audits are carried out by experts/auditors accredited to carry out the audits.

8.3 Relations between evaluators and evaluated entities.

Audit teams do not belong to NG Technologies and are duly authorized to perform the specified controls.

8.4 Topics covered by the reviews

The audit / control can cover all the systems and functions of the Root CA.

8.5 Actions taken following the conclusions of the evaluations

The remarks are considered within a reasonable time and at the latest before the next audit.

Remarks related to key management and security and considered at latest before the next key ceremony session (signature or revocation of AC, publication of LAR).

8.6 Communication of results

The audit is the subject of an internal report submitted to the NG Technologies security committee.

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 Prices

Not applicable. It is an Internal Authority.

9.2 Financial responsibility

Not applicable. It is an Internal Authority.

9.3 Confidentiality of professional data

NG Technologies as responsible for the PKI implements the necessary means to ensure the protection of confidential data including:

- The private key of the root CA;
- The activation data for this key and the HSM used;
- Information and technical documents from the CA.

9.4 Protection of personal data

Not applicable. It is an Internal Authority. It does not process any personal data.

9.5 Intellectual and industrial property rights

Not applicable.

9.6 Contractual interpretations and guarantees

This CA ensures:

- The protection (integrity and confidentiality) of the private key during the generation and throughout the period of validity of the key as well as of the activation data;
- The use of key pairs and certificates for which they were issued, in accordance with the applications defined in this CP in chapter1.4 ;
- The publication of the public information cited in the chapter2.2 of this document, in a sustainable and secure manner;
- Submission to compliance checks carried out by external or internal auditors and the implementation of their recommendations;
- Good documentation of internal operating and use procedures;
- Raising the awareness of trusted staff of their commitments.

9.7 Warranty limit

Not applicable.

9.8 Limitation of Liability

Not applicable.

9.9 Indemnities

Not applicable.

9.10 Duration and anticipated end of validity of the CP

9.10.1 Period of validity

The CA CP must remain in force at least until the end of the life of the last certificate issued under this CP.

9.10.2 Early end of validity

Compliance following an evolution of the CP does not impact the certificates already issued.

9.10.3 Effects of the end of validity and remaining applicable clauses

This CP does not formulate any specific requirement on the subject.

9.11 Individual notifications and communications between participants

Not applicable. This CA is internal and only issues daughter Authorities for NG Technologies.

9.12 Amendments to the CP

NG Technologies is in charge of any modification of this CP. CP can evolve to be consistent with CA. In the event of a major change, the OID must be modified which leads to an early renewal of the CA.

In case of OID change, the new OID must be registered at the Instance Nationale des Télécommunications (INT). The NDCA is informed. The communication to the NDCA includes the change log.

9.13 Dispute Resolution Provisions

Not applicable.

9.14 Competent courts

Not applicable.

9.15 Compliance with laws and regulations

Not applicable.

9.16 Miscellaneous

Not applicable.

9.17 Other provisions

Not applicable.