NG Technologies Remote Trust Services

Certification Practice Statement of the Intermediate Certification Authority Remote Trust CA

Identifier	PKI-CPS-RT-CA
Version	1.2
Description	Certification Practice Statement of NG Technologies Intermediate Certification Authority (RT CA).
Classification	Public
Approval	CEO

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

Historical

Dated	*Version*	*Author*	*Comment*	*Approved by*
10/08/2021	1.0	PKI Committee	Initial version.	CEO
13/07/2022	1.1	PKI Committee	- Added several clarifications regarding accepted documents for natural persons and natural persons representing legal entities (paragraph 4.1). - Specified the size /format of first name, last name and birth date. - Updated paragraph Capacities for business continuity following a disaster to specify the RTO.	CEO
04/08/2022	1.2	PKI Committee	- Fixed a typo in the URL for the secondary download link of the CP documents. - Fixed a typo in the CRL download URL in paragraph 4.10.	CEO

INDEX

1 INTRODUCTION

This document constitutes the Certification Practices Statements (CPS) of the NG Technologies Intermediate Certification Authority designated by the Remote Trust Certification Authority or **NG RT CA**. This Certification Authority is attached to (its certificate is signed by) the Root CA authority of NG Technologies.

RT CA and Root CA are part of **NG Remote Trust Service (NGRTS)** which refers to all the electronic certification and signature services operated by NG Technologies.

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

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 RT CA. NG RT 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.

For certificates holders and/or relying parties this CPS becomes effective and binding by accepting a subscriber agreement ("Conditions Générales d'Utilisation"). The agreement forfeits the consent of the relying party regarding accepting the conditions laid out in this CPS.

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: **2.16.788.2.1.4**

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

NGRTS is made up of several entities and departments.

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

1.3.1 Certification Authority (CA)

Further details are given in the associated CP.

The NG RT CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates.

NG Technologies ensures the availability of all services pertaining to the management of NG RT CA, including without limitation the issuing, revocation, status verification of a certificate, as they may become available or required in specific applications.

1.3.2 Registration Authority (RA)

The Registration Authority (RA) is a component of the PKI, responsible for the identification and authentication of certificate applicants.

1.3.3 Registration Operator (RO)

A registration operator is any natural person appointed by NG Technologies to process registration files when human manual operation is required. Any action performed by the registration operator requires strong authentication to access registration entries.

All actions are traced with the identity, the object of the action and the date (see section **Error! Reference source not found.**).

1.3.4 Delegated Registration Authority (DRA)

The RA may delegate all or part of the registration service to an external entity which will act as a Delegated Registration Authority (DRA).

1.3.5 Delegated Registration Operator (DRO)

A Delegated Registration Operator is any natural person who performs all or part of the verifications necessary for the request for a certificate. It must be attached to a Delegated Registration Authority.

1.3.6 Certificate Holders

The Certificate Holder is the natural person or natural person representing a natural entity.

The Holder has necessarily adhered to the conditions provided for in the “General Conditions of Use of NG Remote Trust Services” of NG Technologies.

In the procedures described in this document, the holder may also be designated by Certificate requester.

1.3.7 Certificate users

Certificate users (or relying parties) trust certificates issued by the CA and / or digital signatures verified using those certificates.

Certificate users can also be private third-party platforms or associated with public administrations or any application that accepts NG Technologies certificates.

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

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

NG RT CA maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

3.1 Naming

Regulation of this is given in the associated CP.

3.2 Initial Identity Validation

Further details are given in the associated CP.

Verification of the identity of the certificate requester (Certificate Holder) is a prerequisite for the validation of any certificate request. The verification concerns the identity of the Holder (legal or natural person) as well as all the attributes that will be part of the certificate or of the activation data (phone number and email).

The verification is carried out based on the establishment of a secure correspondence between the natural or legal person (future) Holder of the certificate and an identity document. In addition to the first and last name, the verification must cover all the attributes that will be included in the certificate.

The identity verification step must make it possible to verify the following elements and to add to the requester file the proof for each element. The output of the initial validation must allow the CA to have proofs of the elements in the table below:

#	Verification	Step	Way	Evidence/Proof support	Delegation
1	Consent of the Applicant and acceptance of the general conditions	Collection of data	Check box on the form.	Trace on the database.	Yes
2	Presence of all required personal data and identity documents	Collection of data	Automatic checks when the form is validated.	The presence of data in the database.	Yes
3	Control of the phone number associated with the request.	Collection of data	Send an OTP code by SMS and enter the code on the form	Trace on the database	No
4	Control of the email address associated with the request by the requester.	Collection of data	Sends an OTP code by email in a confirmation link and click	Trace on the database	No

			on the link by the requester.		
5	Secret PIN code communicated to the requester	Transmission of activation data	Transmission of the PIN code according to the protocol of the ADC component and the entry of the PIN code on this same component.	Trace on the database	No
6	Physical consent of the certificate applicant (at least 18 years old, he is not under threat and justifies all physical faculties for the request and use of his certificate)	Identity verification	Video or Face to Face	Video session or proof of Face to Face.	Yes
7	Acceptance by the Applicant of the personal data that will be added to the certificate (last name, first name, organization)	Identity verification	Video or Face to Face	Video session or proof of Face to Face.	Yes
8	Correspondence between the personal data (nationality, name, first name and date of birth) entered and the identity document used.	Identity verification	Video or Face to Face	Video session or proof of Face to Face.	Yes
9	Correspondence between the physical characteristics of the certificate applicant and the physical characteristics on the identity document used.	Identity verification	Video or Face to Face	Video session or proof of Face to Face.	Yes

3.2.1 Identity verification via electronic channel

The objective of the video identification session is to allow the Certification Authority to verify the identity of the requester and to add the recorded video to the requester file as proof of identity verification.

The identification session must be performed exclusively by NG Technologies or by a DRA approved by NG Technologies.

The identification session is an interactive exchange between the registration authority or the delegated registration authority and the requester.

The result of the video verification (the video and the associated metadata) is considered as an additional supporting document forming part of the certificate request and which is processed under the same conditions as the other supporting documents (archiving).

3.2.2 Identity verification through the face-to-face channel

An operator or a delegated operator performs the verification directly based on an identity document. The document used for the verification must be the same as that included in the electronic supporting documents files.

The NG Technologies operator or the delegated operator must also, during this face-to-face meeting, verify all the other documents forming part of the Certificate request. This verification is done by scanning the necessary documents and checking a box in a checklist.

The responsibility of the Delegated Operator and its organization (DRA) is engaged by affixing its electronic signature to the request.

3.2.3 Identity verification by a DRA

A DRA (Delegated Registration Authority) may use one of the two means of verification above as part of a DRA contract with NG Technologies. The DRA contract must explicitly specify the commitments and the responsibility of the DRA. The commitments include the technical, financial, and operational aspects.

In all cases, NG Technologies verifies the documents/files/proofs used by the DRA for carrying out the identity verification. The format and specification of the documents/files/proofs must conform to the verification requirements used by NG Technologies.

NG Technologies, as the operator of NG RT CA, retains the right to refuse any file on the basis of a real reason which must be communicated to the DRA.

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

A Certificate Holder can make a revocation request at any time through a web interface. The link to this interface is available from the NG Technologies website or from the emails that the holder received when making his request.

The Holder can also call by telephone (the phone number is in the website) or contact NG Technologies through the contact form, to be guided by an operator to make the revocation request.

The Certificate Holder must choose the option "revoke my certificate" (which is public and does not require any authentication), enter the following data:

- His email
- His phone number
- The OTP channel (email or phone)

The holder is informed that this operation is irreversible, and he checks a box to continue the revocation process.

If the data entered is valid (existing email and telephone number, valid certificate, etc.), the client receives an OTP via the channel requested by the client.
The customer is required to enter the following data:

- OTP code
- The reason for revocation (key compromised, data change, unspecified…).

Following the holder's validation, the revocation request is transferred to the Certification Authority. If the revocation request is successful, the customer is notified by email.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate request/application

4.1.1 Origin of a Certificate request

The Certificate request must be made by the Holder. The initial identity validation must be done for the Holder (the person requesting the certificate) and cannot be delegated.

4.1.2 Process and responsibilities for establishing a certificate request

This procedure consists of collecting the personal data as well as the supporting documents necessary for the certificate request.

Certificates of natural persons:

A certificate request must include, at a minimum, the following information:

Information	Type
Certificate type	Choice between “Natural person certificate” (certificate for personal usage) and “Corporate certificate” (Certificate as representative of a Legal entity).
Nationality	Choice from a drop-down list of country codes (ISO 3166-1 alpha-2).
Type of ID	Choice from a drop-down list with the list of accepted documents (see below).
Id number	String of characters. The size and format control should be done according to the type of ID.
ID	PDF or PNG file (s) (image). The number of files depends on the type of identity document.
First name	Character string (Latin letters). Must be identical to the first name on the ID. Must be compliant to the following pattern: "^ [A-zÀ-ÿ][A-zÀ-ÿ- '-]{1,}$". The length must not exceed 63 characters.
Last name.	Character string (Latin letters). Must be identical to the first name on the ID. Must be compliant to the following pattern: "^ [A-zÀ-ÿ][A-zÀ-ÿ- '-]{1,}$". The length must not exceed 63 characters.
Date of Birth	Character string in Date format. Must be identical to the date of birth on the ID. The requester must be older than 18 and younger than 120.
E-mail	Character chain in enamel format.
Phone number	Digital channel in phone format. The size depends on the country.

When using an identity document with personal data written in characters other than Latin, then the requester must use the common transliteration of his name/first name in the request form. The CA operator may reject the request if the transliteration is not correct or not common. In all cases, the requester is invited to confirm the transliteration result during the identity verification step.

Only the following identity documents are accepted:

- Tunisian National Identity Card (CIN): front and back;
- Residence card: front and back;
- Passport: the main page with photo, personal information and MRZ (Machine Readable Zone).

Any identity document must be valid at the request date. The validity range must be explicitly indicated in the document.

Before sending any data to the NGRTS, data collection step includes the acceptance of the General Conditions of Use as well as the CP / CPS which are presented to the applicant (future Holder). Acceptance and consent are indicated by one or more checkboxes.

Collection must be done exclusively via a form hosted by NG Technologies or by a Delegated Registration Authority appointed by NG Technologies. The responsibility of the DRA is engaged in each registration file.

The data transmission channel between DRA and NG Technologies is secured using server authentication (SSH) and an API key for web service exchanges.

NG Technologies only processes electronic documents. No paper document is accepted by NG Technologies. If the DRA accepts paper documents, it must ensure the scanning before sending to NG Technologies. The archiving of paper documents is under his own responsibility.

All documents must be sent in PDF or image format and must be color and good quality documents. The final acceptance of the document (in relation to its quality, its country of issue, the time remaining before its expiry) remains at the sole and exclusive discretion of NG Technologies.

Natural persons representing legal entity

Natural persons representing a legal must be provide the same information described above in addition to the following information:

Information	Type
Organisation name	Character string (Latin characters). The name of the legal entity as it appears in the company registration document.
Nationality of the organisation	Choice from a drop-down list of country codes (ISO 3166-1 alpha-2).
Tax number	Tax number (identifier) of the organization.

The requester must provide the official registration document of the company. The registration document:

- must explicitly mention the information above (with the same spelling or with a common transliteration if it does not use Latin characters).
- must identify the requester as the legal representative of the organization (with the same spelling or with a common transliteration if it does not use Latin characters).
- must be stamped (handwritten or digital signature) by the competent authority.

Currently, "Natural persons representing legal entit" certificates are issued only for organizations registered in Tunisia. Other countries may be supported later.

4.2 Certificate application processing

The issuance of a certificate covers the steps from receiving a certificate request, processing it to issuing the certificate and transferring the certificate to the applicant.

4.2.1 Certificate processing steps

Processing includes the following steps described below:

- Collection of certificate request data from the requester (future holder);
- Verification of request data;
- Modification of request data (if necessary);
- Key pair generation;
- Transmission of Activation Data;
- Identity verification;
- Certificate issuance.

4.2.1.1 Collection of Certificate request data

This procedure consists of collecting the personal data as well as the supporting documents necessary for the certificate request.

See 4.1.2 above for details.

4.2.1.2 Verification of request data

This step consists of verifying the consistency and integrity of the request. Most of the time it is done automatically. Checks include:

- Verification that the request is complete (all the information and documents requested are present);
- Verification of all electronic signatures of all signed documents included in the request;
- Verification of visible electronic seals (CEV) of all documents bearing a 2DDOC seal;

The request can be rejected if any of the above conditions fail. The reason for the failure is communicated to the originator of the request.

4.2.1.3 Modification of the certificate request

If any of the following information is invalid, the operator is authorized to correct it before accepting the request:

- The type of identity document;
- Identity document number;
- The identity document.
- The name (typo error)
- The first name (typo error)

- Date of birth (typo error).

Changing the request requires the following operations:

- Obtain the certificate requester agreement to make the correction and, if necessary, request a new identity document file; the agreement can be in the form of an email exchange.
- The operator makes the correction;
- NGRTS keeps track of the correction by indicating the erroneous information and the identity of the operator who took charge of the correction.

4.2.1.4 Key pair generation

Once a complete and verified certificate request is received by NG Technologies, a new key pair is generated in the NGRTS signing HSM, a tamper proof resistant environment hosted in a secure area with very restricted access. Any physical or logical operation on the HSM requires the presence of at least two persons and the authorization of the CISO. See 5 for further details.

The new key pair is initialized with the activation data (telephone number and PIN code). See below for further details.

4.2.1.5 Transmission of Activation data

The private key is generated in the HSM operated by NG Technologies and is protected by an activation protocol that guarantee that only the certificate holder can activate the private key for signing. The activation protocol is based on typo two authentication factors to allow remote access to his signing key in a secure manner and to ensure sole control of the signing key.

The two factors must be of different families and transmitted through two completely independent channels. NGRTS uses the following two authentication factors:

- A PIN code specific to the signing key. This is the personal code for the use of the certificate. It must be kept secret by the holder.
- An OTP code sent by SMS to the telephone number of the Certificate Holder. It is a one-time code linked to a single signature request (activation request) and which expires after a very limited period (few minutes).

The PIN code transmission procedure is performed exclusively on a secure web interface managed by a web component of NGRTS called "Signer Interaction Component" (SIC). The SIC is a technical component (part of NGRTS) which implements a secure protocol to transmit the activation data to the certificate holder. It ensures that the PIN (or the representation of the PIN) is transmitted encrypted over a dedicated channel. This is not based on the HTTPS connection between the client and the server but a separate cryptographic protocol (ie, even the client and the server cannot decode the PIN code). The PIN code is not transmitted by SMS either as the SMS channel will be used for the OTP in addition to the fact that SMS is no longer considered a secure channel.

4.2.1.6 Identity verification

See 3.2 above.

4.2.1.7 *Certificate issuance*

The issuance of the certificate and its signature by the NG Technologies certification sub-authority requires that all mandatories' conditions are met and have been verified by the CA.

See 3.2 above.

4.2.2 Acceptance or rejection of the request

Regulation of this is given in the associated CP.

4.2.3 Duration

Regulation of this is given in the associated CP.

4.3 Certificate issuance

See 4.2.1 above.

4.3.1 CA actions during certificate issuance

See 4.2.1 above.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The certificate holder/requester will receive a notification at least by email. He may also receive a notification by SMS or via a third-party channel.

4.4 Certificate acceptance

4.4.1 Procedure for accepting the Certificate

Regulation of this is given in the associated CP.

4.4.2 Publication of the Certificate

Regulation of this is given in the associated CP.

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

Not applicable.

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

Not applicable. No re-key is allowed.

4.8 Certificate modification

No modification is authorized by NG Technologies. The Holder must make a new request.

4.9 Certificate revocation and suspension

Regulation of certificate revocation is given in the associated CP.
Further details are given in 3.4
Suspension of certificates is not supported.

4.10 Certificate status services

NG Technologies makes available to User Parties:

- A web server for the provision of CRLs: https://pki.ng-cert.com/repository/public/ng-rt-ca.crl
- OCSP server: https://pki.ng-cert.com/ocsp
- A web server for the provision of CA certificates: http://www.ng-cert.com/repository/public/

Revocation information contain information about the status of Certificates until they expire.

4.11 End of subscription

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.

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.

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
PKI Operator (PO)	Agents involved in administrative tasks related to registration (request or revocation of certificates). A PKI Operator may be a CA Operator (CO) operating at the Certification Authority level, or an RA Operator operating at the Registration Authority (or Delegated Registration Authority) level.
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
Receipt of certificate requests	PO		
Identification and authentication of certificate holders/requesters	PO		
Verification of subscriber authorization	PO		
Verification of documents	PO		
DN verification	PO		
Generation of authorization information	PO		
Receipt and verification of revocation re-quests	PO		
Verification of requests in respect of completeness and correctness	CO		
Storage of documents if required	CO		
Clearance and forwarding of certificate and revocation requests to	CO		

the CA			
Any operation on the cryptographic keys for the CA (generation, revocation, …)	CISO, CTO	Requires the physical presence of at least 2 SB among 5.	After authorization from the CEO and under the supervision of the SIC (Security Information Committee). 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 certificates (for end-entities) and revocation lists	CO		
Certification; initiation of processes for issuance of revocation lists	NGRTS, CO		The operation is automatic with preconfigured frequency. The CO 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 2 SB among 5.	
Physical administration/maintenance	SO		After authorization

or replacement of other systems			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 2 SB among 5.	Based on key ceremony script.
Restoration of backup data for critical systems (HSM)	CISO, CTO	Requires the physical presence of at least 2 SB among 5.	Based on key ceremony script.
Restoration of backup data for other systems	SO		After authorization from the CISO and under the supervision of the CISO or CTO.
Internal review of procedures	CISO, SA		At regular intervals.
Audit	SA (internal and external)		
Issuance of physical authorizations	CISO		
Technical issuance of authorizations	SO		After authorization from the CISO and under the supervision of the CISO or CTO.
Review of implementation of secure development rules	CTO		

5.2.3 Identification and authentication for each role

Identification and authentication for each role is based on the role models as specified in the sections above. Technical access to individual systems is based on user login and password (ISP and an internal password policy is implemented). Critical systems (CA/RA administration systems) require two-factors authentication.

Physical access to any technical systems is regulated by access control measures defined in Physical Access Management and Logical Access Management procedures. These documents are not public but are made available for auditors (external/internal) to verify conformance.

5.2.4 Roles requiring segregation of duties

The following table shows roles requiring separation of duties.

Roles	Incompatible with
CISO	CTO, PO
SO	SA, PO
SA	PO, SO
CTO	CISO, PO
PO	SA, SO, CISO, CTO
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

Archiving can be carried out by NG Technologies on its own servers, or by a third party linked to NG Technologies by a contract containing the same obligations as NG Technologies.

Data to be archived include:

- PCs and CPS documents;
- Certificates and CRLs as issued or published;
- The commitments signed by all the Delegated Registration Authorities;
- The commitments signed by all third-party contractors;
- Proof of identity of holders and, where applicable, of their parent entity;
- The event logs of the various entities of the PKI.

Whenever possible these data/documents are kept in an electronic form. The main requirement to keep only an electronic form of a document, is the availability of an electronic signature/timestamp on the document ascertaining its authenticity and integrity.

Technical data (logs, certificate request data…) are collected and archived in a secure way. Integrity and authenticity are guaranteed using technical ways (log system, database…).

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.

The restoration delays depend on the nature of the disaster and the target service. In case of a extremely major disaster, the revocation service is designed to be restored in less than 6 hours. The issuance of new certificates service is designed to be restored in less than 3 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.

6.1.1.2 Holders Keys

Key pairs are generated on the HSM (Hardware Security Module) hosted by NG Technologies. The generation is done exclusively by the system of NGRTS in the secure environment and using the HSM.

NGRTS does not manage and certify keys generated out of NG Technologies secure environment.

Private Keys are generated on the HSM (Hardware Security Module) hosted by NG Technologies but the holder keeps the sole control of the usage of this key. See 4.2.1.5 for further details.

6.1.2 Transmission of the private key to the Holder

The private key is not transmitted to the Holder. The Holder is given activation data based on two authentication factors to access his key (see 4.2.1.5 for further details).

6.1.3 Transmission of the public key to the CA

The generation of the key pair (public and private) is made internally by the NGRTS PKI software. No transmission from outside the CA.

The generation of the key pair, the transmission to the CA and the signing of the certificate by the CA key are all steps performed by the NGRTS PKI software without taking any external parameters.

6.1.4 Transmission of the CA's public key to the Relying Parties

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 = 2 out of n = 5);
- 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 4.2.1.5 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

6.4.1 Generation and installation of activation data

6.4.1.1 Generation and installation of the activation data corresponding to the private key of the CA

Regulation of this is given in the associated CP.

6.4.1.2 Generation and installation of activation data corresponding to the holder's private key

Regulation of this is given in the associated CP.

6.4.2 Activation data protection

6.4.2.1 Protection of activation data corresponding to the private key of the CA

See 6.2.2 and the associated CP for further details.

6.4.2.2 Protection of activation data corresponding to the holder's private key

See 4.2.1.5 and the associated CP for further details.

6.4.3 Other aspects related to activation data

Not applicable.

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.