NG Technologies Remote Trust Services

Certification Policy of the Intermediate Certification Authority - Remote Trust CA

Identifier	PKI-CP-RT-CA
Version	1.2
Description	NG Technologies Intermediate Certification Authority (RT CA) Certification Policy.
Classification	Public
Approval	CEO

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

Historical

Dated	***Version***	***Author***	***Comment***	***Approval***
10/08/2021	1.0	PKI Committee	Initial version	CEO
15/05/2022	1.1	PKI Committee	Deleted the specific handling (using a dash) for “compound names” (paragraph 3.1.4).	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 URL of the form to request revocation	CEO

INDEX

Acronyms

- **NDCA:** National Certification Agency (Agence Nationale de Certification Électronique, ANCE in french)
- **ANSI:** National IT Security Agency (Agence Nationale de Sécurité Informatique)
- **CA:** Certification Authority (AC in French)
- **CP:** Certification Policy
- **RA:** Registration Authority (AR in French)
- **CISO:** Chief Information Security Officer
- **CGU:** General conditions of use
- **CPS:** Certificate Practices Statements
- **CSR:** Certificate Signature Request
- **DPC:** Certification Practices Statements
- **DRA:** Delegated Registration Authority
- **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
- **NGRTS**: Next Generation Remote Trust Services
- **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 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 (NG Root CA).

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

1.2 Document 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 policy is identified by the OID: **2.16.788.2.1.2**

Any revisions to this document will be noted in the history section above.

Any change of OID will be mentioned in this section.

1.3 Intervening entities

NGRTS is made up of several entities and departments.

1.3.1 Certification Authority

A Certification Authority (CA) means the authority in charge of creating, issuing, managing, and revoking Certificates under the Certification Policy.

In this document the term RT CA refers to the intermediate Certification Authority of NG Technologies (sometimes simply referred to as the CA in the text).

The term Root CA designates the Primary Authority of NG Technologies whose certification policy is described in another document.

1.3.2 Registration Authority

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

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

1.3.3 Registration Operator

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 5.4).

1.3.4 Delegated Registration Authority

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

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 holding the Certificate.

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

1.4.1 Applicable areas of use

1.4.1.1 Key pairs and holders’ certificates.

This CP deals with key pairs and certificates intended for the categories of Certificate holders (see 1.3.6 above), so that these holders can authenticate and / or electronically sign data (documents, messages).

Regarding the authentication function, it can be authentication within the framework of access control to a server or an application, or authentication of the origin of data within the framework of electronic messaging.

Regarding the signature function, this provides, in addition to the authenticity and integrity of the data thus signed, the manifestation of the signatory's consent as to the content of this data.

No other use of the key pair is authorized.

1.4.1.2 Key pairs, CA certificates and component certificates

The CA has only one key pair and the corresponding Certificate is attached to a higher-level CA (Root CA of NG Technologies).

The different internal keys in NGRTS are listed below:

- The CA signing key is used to sign the certificates generated by the CA as well as the information on the status of the Certificates (CRL and, optionally, OCSP responses);
- The infrastructure keys, used by the systems involved in the PKI for authentication, signing event logs, encryption of data exchanged or stored within NGRTS, etc.;
- The control keys, assigned to NG Technologies personnel or personnel authorized by NG Technologies in order to authenticate themselves to the various systems, to sign and / or encrypt messages or data exchanged, etc.

1.4.2 Areas of use prohibited

Any use not mentioned in the paragraph 1.4.1 above is prohibited.

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 CP

NG Technologies via internal and external audits.

1.5.4 CP compliance approval procedures

External audits are also regularly carried out with audit reports. See paragraph Compliance audit and other assessments.

2 RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION TO BE PUBLISHED

2.1 Entities responsible for making information available

NG Technologies publishes information relating to the service it provides.

NG Technologies publishes the valid CP and its previous versions as well as the General Conditions of Use.

This publication is made on a dedicated page on the NG Technologies website dedicated for NGRTS: http://www.ng-cert.com/repository/public/

These documents are published as well on NGSign web site: http://www.ng-sign.com/

The links above are made public starting from the date of the public launch of the certificate issuance service.

NG Technologies may temporarily use other communications channels in case of unavailability of this main channel. In this case, NG Technologies must inform all parties concerned of the temporary channels used.

2.2 Publication of certification information

NG Technologies undertakes to publish at least:

- The applicable CP /CPS documents.
- The general conditions of use of the certification services.
- The CRLs published according to the requirements of the CP applicable to Certificates.
- Certification Authorities certificates.

NGRTS uses the page http://www.ng-cert.com/repository/public/ as the main page for the publication.

CP/CPS documents are published as well in NGSign web site: http://www.ng-sign.com/ .

The links above are made public starting from the date of the public launch of the certificate issuance service.

2.3 Publication deadlines and frequencies

The deadlines and frequencies of publication vary according to the information concerned:

- CRLs are published daily.
- CA Certificates are distributed or posted online before use.
- The CP, CPS and General Conditions of Use are published after each update. All history is also published.

2.4 Access control to published information

The information published is made available to the public and free to read. See section 2.1 for publication channels.

Modifications of this information are limited to authorized persons and under the control of the NG Technologies team in charge of NGRTS.

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 CA and the Holder are identified by an explicit name, the "Distinguished Name" (hereinafter referred to as "DN") of the X.501 type. The DN fields and their semantics are shown in the table below.

Certificates of natural persons: Certificates of natural persons issued by the CA include the following fields:

Field	Obligatory?	Field semantics	Verified by the RA/DRA?
CN	Yes	Last name and first name of the natural person (see givenName and surName).	Yes
C	Yes	Nationality	Yes
givenName	Yes	First name	Yes (must be in accordance with the identity document)
surname	Yes	Last name	Yes (must be in accordance with the identity document)
O	No	Designation of the legal person to which the natural person is attached	Yes
OU	No	Unique legal identifier of the legal person to which the natural person is attached, structured according to ETSI 319 412-1	Yes
EmailAddress	Yes	Applicant's email address	Yes (Automatic verification by the RA)
serialNumber	Yes	The unique serial number assigned by the CA	N / A

Natural persons representing legal entity: Certificates issued to natural person representing a legal entity (certificate with professional attributes):

Field	Obligatory ?	Field semantics	Verified by the RA/DRA?
CN	Yes	Last name and first name of the natural person (see givenName and surName).	Yes
C	Yes	Nationality	Yes
givenName	Yes	First name	Yes (must be in accordance with the identity document)
surname	Yes	Last name	Yes (must be in accordance with the identity document)
O	Yes	Designation of the legal person to which the natural person is attached	Yes
OU	Yes	Unique legal identifier of the legal person to which the natural person is attached, structured according to ETSI 319 412-1	Yes
EmailAddress	Yes	Applicant's email address	Yes (Automatic verification by the RA)
serialNumber	Yes	The unique serial number assigned by the CA.	N / A

3.1.2 Explicit names

The names chosen to designate the Certificate Holder must be explicit, they must make it possible to directly identify the Certificate Holder.

3.1.3 Anonymization or pseudonymization of Holders

The anonymization and pseudonymization of the holders are prohibited.

3.1.4 Rules for interpreting different forms of names

No interpretation is to be made of the information entered in the "Subject" field of the Certificates.

This information is established by the RA/DRA and is essentially based on the following rules:

- Names in Arabic are converted to Latin letters according to common usage. The conversion must be validated by the Certificate Holder. In case of ambiguity, the official birth certificate in French may be requested.

- All the characters are in printableString or UTF8String format, ie without accents or characters specific to the French language and in accordance with the X.501 standard;

3.1.5 Uniqueness of names

The same DN cannot be assigned to different holders.

3.1.6 Identification, authentication, and role of trademarks

Certificate Holders declare that they hold the intellectual property rights associated with the names, trademarks, domain name or other distinctive sign contained in their Certificate. The CA does not check these rights but authorizes itself to reject a Certificate request or to revoke a Certificate in the event of a dispute over these distinctive signs. The CA disclaims all liability in the event of unauthorized use of elements protected by intellectual property rights.

3.2 Initial identity validation

The registration of a holder can be done either directly with NG Technologies RA or via an authorized Delegated Registration Authority (DRA). In the latter case, the DRA must be previously registered by the RA and have signed a contract with NG Technologies.

The same procedure, same documents and same checks must be carried out in both cases. The CA will only generate the certificate by submitting a complete file of supporting electronic documents including the acceptance of the General Conditions of Use.

The list of supporting documents is published on the NG Technologies PKI website (see section 2.1for communication channels). All documents must be received in electronic format.

3.2.1 Method to prove possession of the private key

Not applicable.

3.2.2 Validation of the identity of an organization

Same requirement in section 3.2.3 below.

The specificity is only in the requirement of additional supporting documents for the organization.

3.2.3 Validation of an individual's identity

Validation can be done by the RA or by a DRA previously authorized by the RA. In both cases, the identity validation procedure is the same.

The Certificate Holder (natural or natural person representing legal person) must provide the information and documents useful to justify his identity and the elements he intends to include in the Certificate. Only the elements strictly necessary for the establishment of the Certificate are required by the CA and requested by the RA or DRA.

All documents must be received in electronic format.

The Holder is notified that a copy of the proof of identity documents will be securely kept by the RA in the Holder's registration file.

3.2.4 Unverified holder information

All information provided by the Holder is verified by the RA or DRA. The verification is mainly based on the supporting documents provided by the certificate applicant.

The email is verified by sending an OTC (One Time Code) to the email address for validation.

The phone number is verified by sending an OTC by SMS for validation.

3.2.5 Validation of the authorization of the applicant

The RA verifies the authorization of a natural person to represent a legal person during the validation of the identity of the Holder.

3.2.6 Interoperability criteria

Not applicable.

The CA has no recognition agreement with another CA.

This article will be modified upon establishment of such an agreement.

3.3 Identification and validation of a key renewal request

3.3.1 Identification and validation for a current renewal

The holder may be notified of the expiration of his certificate 1 month then 2 weeks before the expiration. During the last 5 days, the Holder may receive a warning email per day. The holder is invited to provide a new request.

Automatic renewal is not supported.

3.3.2 Identification and validation for renewal after revocation

Not applicable. No renewal is allowed after revocation.

3.4 Identification and validation of a revocation request

The RA or DRA authenticates the revocation requestor, based on the information contained in the registration file in the case of a request for revocation of a Certificate intended for a natural person. It also verifies the authorization of the applicant in accordance with a request for revocation of a Certificate intended for a legal person.

The revocation request must be sent through an electronic channel made available to Certificate Holders accessible from https://app.ng-cert.com/ngcert/.

4 OPERATIONAL REQUIREMENTS ON THE LIFE CYCLE OF CERTIFICATES

4.1 Certificate request/application

4.1.1 Origin of a Certificate request

The Certificate request must be made by the Holder.

4.1.2 Process and responsibilities for establishing a certificate request

The Certificate request includes the Holder's identification data. These identification data are transmitted under its sole responsibility.

Three entities are involved in the process:

- The Applicant (future Certificate Holder);
- The Registration Authority (or the Delegated Registration Authority) who receives and processes the certificate request;
- The Certification Authority

The process of requesting a certificate requires the following steps:

1. Presentation of the General Conditions of Use and consent of the Requestor;
2. The applicant provides to the RA (or DRA) the data and documents to present a “Certificate Holder File”. As such, he guarantees the accuracy of the information provided and must provide the RA (or DRA) with all the necessary elements of the registration file;
3. The RA validates the email and telephone number of the future certificate holder;
4. The RA generates the key pair on an HSM, validates the authentication factors and sends the activation data to the Requestor;
5. The Applicant validates his activation data;
6. The CA validates the requester data and verifies the identity of the applicant (see section 3.2.3);
7. The CA generates the certificate

4.2 Processing a Certificate request

4.2.1 Execution of the request identification and validation process

Any certificate request must be processed by the Backoffice of the NG Technologies Registration Authority. The front (direct interactions with the Holder) can be done by NG Technologies or a Delegated Registration Authority. In all cases, the final request is received by CA of NG Technologies which alone can decide on its acceptance or rejection.

The identification process depends on the channel used to verify the identity. Two channels are allowed:

- The physical Face to Face;
- A video session.

The conditions and prerequisites for using this channel are communicated to the Requestor who can refuse them.

Upon receipt of the request, the RA (or DRA) performs the following operations:

- Validate the identity of the future holder;
- Check the consistency of the supporting documents presented;
- Ensure the existence and validity of the applicant's request;
- Make sure that the future holder is aware of the applicable terms and conditions for the use of the certificate.

The “email” and “phone number” attributes are always validated only by the RA on the basis of challenges sent on these channels. These validations cannot be delegated to the DRA.

The other checks can be delegated to DRA. The RA can always redo a verification based on the received documents.

If the request is not complete (e.g missing document), the applicant is contacted to complete their request. Whatever action is taken on the request, the requester is informed. The exchanges are made on the email and the telephone number which have already been validated. If the registration procedure is stopped before the validation of these two factors, the request is rejected.

Once all the verification operations have been carried out, the RA sends the certificate generation request to the appropriate CA function (see section 1.3.1).

The CA keeps an electronic copy of the entire request received (including all requester documents).

The DRA can keep a copy. Only the copy archived by the CA is valid in any subsequent verification.

4.2.2 Acceptance or rejection of the request

The CA processes the request as soon as it is received. If the application is rejected during one of these stages, the applicant will be informed as soon as possible.

4.2.3 Duration

The deadline for generating a certificate is a maximum of three working days from receipt of a complete request.

4.3 Certificate issuance

4.3.1 Actions of the CA concerning the issuance of the Certificate

The CA creates a Certificate at the end of the Certificate request validation process defined in the previous section. The Certificate issued complies with the information contained in the Certificate request and with the profile defined in the section 7.1.

Once the certificate has been generated, the Holder is notified by email.

4.3.2 Notification by the CA of the issuance of the Certificate

See section 4.3.1 above.

4.4 Acceptance of the Certificate

4.4.1 Procedure for accepting the Certificate

The certificate holder declares acceptance of the certificate before finalizing his request by accepting the general conditions of use as well as the CP / CPS.

4.4.2 Publication of the Certificate

Certificates are public and accessible using NG Technologies web services.

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

The authorized use of the holder's key pair and of the associated certificate is indicated in the certificate itself, via the extensions concerning the uses of the keys.

The Holder undertakes to use the Certificate in accordance with:

- To this Certification Policy;
- Under the terms of the General Conditions of Use to which he must consent before obtaining the certificate;
- For the uses provided for in its certificate request (uses applied in the content of the KeyUsage extension in the certificate).

The Relying Parties agree to the terms of the User Agreement before any use of NG Technologies Services.

The User Parties are required to:

- Determine that the use of the Certificate complies with the conditions provided for by the CP (see section**Error! Reference source not found.**);
- Determine that the Certificate is used in accordance with the Key Usage extension defined therein;
- Check the status of the Certificate (not expired and not revoked).

NG Technologies excludes all liability in the event of use of the Certificate for a use that does not comply with: this CP, the uses authorized in the certificate, the general conditions of use or any other specific agreement concluded between the Holder, the User Party and the Certification Authority.

4.6 Renewal of a Certificate

Not applicable. No renewal is allowed.

4.6.1 Possible reasons for renewing a Certificate

Not applicable.

4.6.2 Origin of a renewal request

Not applicable.

4.6.3 Procedure for processing a renewal request

Not applicable.

4.6.4 Notification to the Holder of the establishment of the new Certificate

Not applicable.

4.6.5 Procedure for accepting the new Certificate

Not applicable.

4.6.6 Publication of the new Certificate

Not applicable.

4.6.7 Notification by the CA to the other entities of the issuance of the new Certificate

Not applicable.

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

Not supported. The holder must make a new request.

4.7.1 Possible causes of changing a key pair

Not applicable.

4.7.2 Origin of a request for a new Certificate

Not applicable.

4.7.3 Procedure for processing a request for a new Certificate

Not applicable.

4.7.4 Notification to the Holder of the establishment of the new Certificate

Not applicable.

4.7.5 Procedure for accepting the new Certificate

Not applicable.

4.7.6 Publication of the new Certificate

Not applicable.

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

Not applicable.

4.8 Modification of the Certificate

No modification is authorized by NG Technologies. The Holder must make a new request (see section4.2).

4.8.1 Possible causes of modification of a Certificate

Not applicable.

4.8.2 Origin of a request to modify a Certificate

Not applicable.

4.8.3 Procedure for processing a request to modify a Certificate

Not applicable.

4.8.4 Notification to the Holder of the establishment of the modified Certificate

Not applicable.

4.8.5 Procedure for accepting the amended Certificate

Not applicable.

4.8.6 Publication of the amended Certificate

Not applicable.

4.8.7 Notification by the CA to the other entities of the issue of the modified Certificate

Not applicable.

4.9 Revocation and suspension of Certificates

A Certificate issued by NG Technologies can only be in one of the following three states: valid, expired or revoked. Suspension is not permitted.

4.9.1 Possible causes of revocation

The revocation of a Holder's certificate can be linked to one of the following reasons:

- The Holder's information appearing in his Certificate is not or no longer accurate, before the normal expiration of the Certificate;
- The information appearing in the request turns out to be fraudulent;
- The Holder has not complied with the rules for using the Certificate or the General Conditions of Use of NGRTS services;
- The Holder's private key is suspected of being compromised;
- The Holder (or his legal representative) makes an explicit request;

When one of the above circumstances occurs and the CA becomes aware of it, the relevant Certificate is revoked and placed in the Revoked Certificate List (CRL).

4.9.2 Origin of a revocation request

The Holder or the legal representative of an entity whose name is present in the certificate may submit a request for revocation.

The NG Technologies reserves the right to revoke any certificate that has not been used in accordance with the General Conditions of Use.

4.9.3 Procedure for processing a revocation request

The validation of the request by the CA must include the verification of the origin of the request and its admissibility. Only requests received according to the provisions of section 3.4 are accepted and processed without delay.

The CA informs the Holder of the effective revocation of the Certificate and of the change of status.

Any revocation is final.

4.9.4 Time allowed for the Holder to formulate the revocation request

The Holder must make the revocation request without delay as soon as he becomes aware of one of the reasons justifying the revocation.

4.9.5 Deadline for the CA to process a revocation request

Revocation requests are processed from the effective authentication of the requester and the acceptance of the request.

The delay is 3-hours if the Holder (or his legal representative) uses the revocation code received when generating the certificate to validate the revocation request

The delay is 16 hours if the Holder (or his legal representative) follows another electronic channel.

Once processed (confirmed), the updated revocation status is published after at most 60 minutes.

4.9.6 Revocation verification requirements by Relying Parties

The Relying Parties are required to check the status of the Certificates and the corresponding chain of trust. The method used (CRL or OCSP) is at the discretion of the user according to the constraints of his technical environment.

4.9.7 Frequency of establishment of CRLs

A new CRL is published every 24 hours or every 3 hours when a new certificate is revoked. In the case of the presence of several revocation requests, the update and publication of a new CRL can be performed for each group of revoked certificates without exceeding 3 hours after the effective revocation of a certificate.

4.9.8 Maximum time limit for publication of a CRL

A new CRL is published no later than 30 minutes after its generation.

4.9.9 Availability of an online verification system for the revocation and status of Certificates

NG Technologies makes available to User Parties both an OCSP service and a CRL download link.

4.9.10 Requirements for Online Verification of Certificate Revocation by Relying Parties

See section 4.9.6.

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

On the compromise or suspicion of compromise of a private key, the Holder must immediately formulate his request for revocation by one of the means of the section 3.4.

In the event of a compromise of the CA's private key, the information is disseminated on all NG Technologies public channels (website and social networks). All certificates signed by this key are immediately revoked.

All holder are immediately informed using the emails used to make the requests.

4.9.13 Possible causes of a suspension

NGRTS does not allow the suspension of certificates.

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 on the period of suspension of a Certificate

Not applicable.

4.10 Information function on the status of Certificates

4.10.1 Operational characteristics

NG Technologies makes available to User Parties:

- A web server for the provision of CRLs
- OCSP Server
- A web server for the provision of CA certificates

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

4.10.2 Function availability

The web servers above are available 24/7.

4.10.3 Optional devices

Not applicable.

4.11 End of the relationship between the Holder and the CA

The relationship between the Holder and the CA systematically ends when the certificate expires or is revoked.
The relationship between the Holder and NG Technologies may continue if the Holder has subscribed to other services on the NG Technologies platform.

4.12 Key escrow and recovery

NG Technologies does not carry out any key escrow.

4.12.1 Key escrow policy and practices

Not applicable.

4.12.2 Session key encapsulation recovery policy and practices

Not applicable.

5 NON-TECHNICAL SECURITY MEASURES

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 will be made available during audits and validation of conformance.

5.1 Physical security measures

5.1.1 Geographic location and site construction

The CA hosts its services in secure premises. These sites and premises have physical security mechanisms to ensure strong protection against unauthorized access.

5.1.2 Physical access

The areas hosting the computer systems of NG Technologies' NGRTS platform are physically protected against unauthorized external access. This includes all software and hardware components.

The list of personnel authorized to access it is maintained by the NG Technologies ISC and is limited to the strict need for the proper functioning of the service. Access by authorized personnel is controlled by physical and registered means.

5.1.3 Power supply and air conditioning

Emergency measures are implemented so that an interruption of the electrical supply service, or an air conditioning failure does not affect the commitments made by the CA in terms of availability.

5.1.4 Exposure to water damage

The definition of the security perimeter considers the risks inherent in water damage. Protection measures are implemented by the host to counter residual risks.

5.1.5 Fire prevention and protection

Accommodation areas are protected against fire (automatic detection and extinguishing). The distribution of machines also ensures maximum availability of services.

5.1.6 Media storage

The media containing saved or archived data are kept with a level of security at least equal to that of the systems which generated them.
For more guarantees, different types (or models) of media storage devices are used for the same data.

5.1.7 Waste disposal

Information stored on data carriers will be destroyed in an appropriate manner. Data stored on paper will be destroyed by the available document shredders.

5.1.8 Offsite backup

In order to enable disaster recovery in accordance with its commitments, the CA sets up backups of critical information and functions off the production site. The CA guarantees that the backups are carried out by people with Trusted Roles. The CA ensures that the backups are exported off the production site and benefit from measures for the protection of confidentiality and integrity. The CA ensures that the backups are tested on a regular basis to ensure that the measures of the business continuity plan are met.

5.2 Procedural security measures

5.2.1 Trusted roles

The administration and operation of all NGRTS systems is entrusted to several key individuals with one of the roles listed below. The assignment of roles is under the control of the ISC. Additional roles (system administrator, database administrator…) may be involved under the supervision of the ISC.

Chief Information Security Officer	He is responsible for implementing the security policy for NGRTS hardware and software components. It manages physical access controls to system equipment. He is responsible for analyzing the event logs in order to detect any incident, anomaly, attempted compromise, etc. It is also responsible for the implementation (security aspects) of this certification policy and the declaration of associated certification practices.
Chief Technical Officer	He is in charge of 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.).
Auditor	He is authorized to audit the archives and all audit data of NGRTS components. May be sub-contractor.
Secret bearer	He ensures the confidentiality, integrity and availability of the secret shares entrusted to him

5.2.2 Number of people required per task

Any administration operation on the CA security equipment requires the presence and the validation of at least 2 persons among five persons. In addition, the physical access to the CA equipment requires formal authorization from the CISO and must have been declared in the access accreditation matrix.

5.2.3 Identification and authentication for each role

The assignment of one of the roles mentioned above requires verification of the identity and of the data transmission channel giving the access associated with the role.
The allocation of secrets (cards, passwords, etc.) associated with one of these roles is done face to face during a ceremony with the presence of the CISO and internal auditor and with an output signed record.

5.2.4 Roles requiring segregation of duties

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

The following accumulations are prohibited:

- Security Officer / Technical manager
- Auditor / Any other role (except secret bearer)

5.3 Safety measures for personnel

5.3.1 Qualifications, skills and authorizations required

Chief Information Security Officer and Chief Technical Officer manager have at least 5 years of experience each in his specialty.

Auditors are qualified for security audits.

Secret bearers are employees of NG Technologies with permanent contracts.

5.3.2 Background check procedures

Before the appointment of a person to a Role of Confidence, the CA verifies his criminal record and professional skills, in order to validate his suitability for the role. In addition to the standard supporting documents forming part of the personal file (diplomas, certificate, etc.), the CA verifies, before any attribution of a trusted role, bulletin N ° 3; or any equivalent document for foreigners; to verify that the criminal record does not present any offense in contradiction with the role in question.

These checks are carried out and reviewed regularly.

5.3.3 Initial training requirements

An internal training period precedes any access to any software or hardware component of NGRTS.

5.3.4 Continuing education requirements and frequency

Each change in systems, procedures or organizations is the subject of information or training for involved persons to the extent that this change impacts their work.

5.3.5 Frequency and sequence of rotation between different assignments

Not applicable.

5.3.6 Sanctions for unauthorized actions

In the event of a proven or suspected fault of a key person in the performance of his duties, the CA denies him access to the systems and, if necessary, takes all appropriate disciplinary sanctions.

5.3.7 Requirements for the staff of external service providers

The requirements vis-à-vis external service providers are contractualized. External service providers are subject to the same security and rigor requirements as NG technologies staff.

5.3.8 Documentation provided to staff

Document’s security rules and procedures are subject to the approval of the Information Security Committee. Safety rules are communicated to staff when taking up a post, depending on the role assigned to the worker.
The persons called upon to occupy an operational role within the CA have access to the corresponding procedures and are required to comply with them.

Shared documents include but is not limited to:

- Information Security Policy (ISP)
- Internal IT Charter
- Internal Regulation Rules
- Certification policies CP) ans Practice Statement (CPS)
- Security Procedures (physical access, logical access, IT resources usage…)

The role of the employee and the classification level of the document is considered before communicating any document.

5.4 Audit data compilation procedures

Any action on a hardware or software component results in an entry in an audit log and/or ceremony report. The audit log is archived in electronic format. Ceremony reports are archived as hard (paper) copies.

The audit log is made up of the log files automatically generated by each software component and audit sheets completed during any operation on a hardware component.

The time used for the provision system date is be synchronized with UTC at least once every 24 hours.

5.4.1 Type of events to record

At least the following events are recorded:

- All the events related to registration (certificate request);
- All events related to the CA key life cycle;
- All events related to the life cycle of certificates issued by the CA, including events related to revocation;
- All the events of the different components of the CA (server start-up, network access, etc.).

These logs make it possible to ensure the traceability and accountability of the actions carried out, in particular in the event of a request from a judicial or administrative authority. The CA describes in its internal procedures the details of the events and the recorded data. Each entry (event) must include the date of the execution of the event.

5.4.2 Processing frequency of event logs

The event logs are systematically used in the event of an abnormal event being reported.

5.4.3 Retention period for event logs

Event logs are kept for a period of 9 years. This guarantee to keep records related to any specific key/certificate for at least 7 years after certificate expiration.

5.4.4 Protection of event logs

Access to the log requires specific access rights. These rights are communicated under the control of the Information Security Committee. These logs are not editable.

5.4.5 How to Back Up Event Logs

Logs are backed up and regularly copied to an external system. The external system is hosted in a secure room with access control.

5.4.6 Event log collection system

An automatic system for collecting event logs is set up. This system guarantees the integrity and availability of these event logs.

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

No notification when recording events.

5.4.8 Vulnerability assessment

The event log files are checked regularly. Upon suspicion of an anomaly or unauthorized access, the logs are immediately checked.

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:

- PCs and DPCs;
- 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 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

Whatever their medium, the archives are protected in integrity and are only accessible to authorized persons. These archives are searchable and exploitable throughout their life cycle and are kept in a secure environment.

5.5.4 Archive backup procedure

A regular backup of data/records specified in sections 5.4.1 and 5.5.1 is made in a regular frequency. Backup are done in respect to RTO (Recovery Time Objective) and RPO (Recovery Point Objective) goals defined in NG Technologies Backup procedures.

Backup media are stored in an appropriate way outside the main IT room.

5.5.5 Data timestamp requirements

The system date (Second / Minute / Hour / Day / Month / Year /) is used to date all events and electronic data (a creation date is associated with each document).

The time used for the provision of system date is be synchronized with UTC at least once every 24 hours.

No cryptographic time stamp requirement.

5.5.6 Archives collection system

An internal archive collection system is used.

5.5.7 Archive recovery and verification procedures

The time taken to retrieve an entry in the archive depends on its medium (hard or electronic) and on its age. This deadline is technical and under the control of the CA.

5.6 Change of CA keys

The CA does not have an automatic key renewal procedure; however, the CA must generate a new key pair and request a Certificate from the Root CA before the expiration of the current CA Certificate validity. This renewal must be done at the latest 2 years before the end of the expiry of the CA certificate. The old key continues to be used only to sign CRLs.

5.7 Recovery following compromise and disaster

5.7.1 Reporting and handling procedures for incidents and compromises

The CA sets up procedures and resources for reporting and handling incidents. These means make it possible to minimize damage in the event of an incident.

The CA sets up a response plan in the event of a major incident, such as a compromise of its publication mechanisms or its Certificate issuance mechanism.

A major incident, such as a loss, suspected compromise or theft of the CA's private key is immediately notified to the ISC Committee, which, if necessary, may decide to revoke the CA.

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

In case, the main site is still operational, hardware/software/data redundancy allows fast recovery.

In all other cases, a continuity plan is put in place to meet the availability requirements of the different components of the CA.

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

The compromise of a CA key immediately results in the revocation of Certificates issued using this key. In this case, the various actors and entities concerned will be warned of the insecure nature of the CRL or certificates signed by the compromised key of the CA. Similar measures are taken if the robustness of the algorithm used or that of the parameters used by the AC becomes insufficient for the uses of the AC.

5.7.4 Capacities for business continuity following a disaster

Following a disaster, the resumption of certificate issuance activity is carried out in accordance with NG Technologies' business continuity plan.

5.8 End of life of the CA

5.8.1 Activity transfer

Transfer is not allowed. The transfer can only be done at the level of the Root Certification Authority.

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 the shutdown to certificates holders and to the people and organizations affected by the plan;
- The revocation of all certificates issued that are still valid at the time of the decision to stop the activity;
- Activation of the procedure for destroying the CA's private key;
- Activation of the the provisions necessary for the continuity of archiving of archived data (see section 5.5.1)
- Destruction of all personal data in the presence of a representative of the National Regulatory Authority.

This plan is checked and kept up to date on a regular basis.

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

The generation of the CA keys is carried out in a secure environment (see section 5) during a formal key ceremony.

Generation takes place during a formal key ceremony following a ceremony script previously established. At least the following people must be present during the ceremony:

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

The generation is done exclusively in the dedicated HSM of the CA and in compliance with the requirements of this PC.

6.1.1.2 Holders Keys

Key pairs are generated on the HSM hosted by NG Technologies. The generation is done exclusively by the system of NGRTS in the secure environment.

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

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 section 6.2.8).

The two factors must be of different families and transmitted through two completely independent channels.

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.

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

The CA's public key can be downloaded from the NG Technologies website in a form of an X.509 certificate. The download link is displayed in a table listing all NGRTS CA certificates. In front of each link, the checksum is also displayed to allow verification of integrity.

6.1.5 Key sizes

The RSA key size of the CA certificate is 4096.

The Holder may have an RSA or ECDSA signing certificate. In the first case, the RSA key size is 2048. In the second case, the ECDSA key size is 256 or 384.

These sizes can evolve according to the cryptographic evolution or the changes in the legal framework.

6.1.6 Checking the generation of key pair parameters and their quality

The CA uses certified equipment (see Sect. 6.2.11) and algorithms whose parameters meet the appropriate security standards.

6.1.7 Objectives of the use of the key

The use of the private key of the CA and the associated certificate is strictly limited to the signing of certificates and CRLs.

Use of the holder's private key and associated certificate is strictly limited to authentication and signature services (see section1.4.1 and 4.5).

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 cryptographic modules used by NGRTS, for the generation and the implementation of the signature keys of the CA or the signature keys of the Holders, are certified hardware cryptographic modules meeting the requirements of the section 6.2.11.

NG Technologies ensures the security of these modules throughout their life cycle. In particular:

- Ensure their integrity during their transport from the supplier;
- Ensure their integrity during their storage prior to the key ceremony;
- Ensure that signature key activation, backup and restoration operations are carried out under the control of at least two staff with Trusted Roles (see section 5.2.1)
- Make sure they are in good working order;
- Ensure that the keys they contain are destroyed when they are de-commissioned.

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.

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

Private keys are backed up in encrypted form and with an integrity control mechanism. These backup copies have the same level of security as the original private key.

The encryption and decryption operations are performed inside the cryptographic module and require the intervention of 2 secret bearers having trusted roles.

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

The CA's private keys are exported only to make backup copies (see section 6.2.4 above).

The holder’s private keys are exported encrypted according to the backup procedures on the main site and the backup site.

6.2.7 Storage of the private key in a cryptographic module

The private keys of the CA are stored encrypted by a key in a cryptographic module. For back-up purposes, a copy is made outside a cryptographic module subject to compliance with the measures in section 6.2.4 above.

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).

6.2.8.2 Holders' private key

The activation of a holder's private key is done following the validation of two authentication factors under the exclusive control of the Holder.

Activation is part of the certificate request procedures (see section 4.1). When the key pair is generated, the two authentication channels are selected by the Holder and validated by the RA (or DRA). The activation channels are validated using challenges before validating the certificate request. The list of authentication factors and the possible combination are presented to the Applicant in the General Conditions of Use.

Activation data is secret data transmitted to the Holder in order to guarantee that he is the sole owner. The data is transmitted through at least two completely independent channels to ensure that the compromise of a single channel does not allow all activation data to be recovered.

6.2.9 Private key deactivation method

6.2.9.1 CA private key

The deactivation of the CA private keys in a cryptographic module is automatic as soon as the environment of the module changes: shutdown or disconnection of the module, disconnection of the operator, etc.

6.2.9.2 Holder's private key

The private keys of the Holders are deactivated in the cryptographic module. Activation is under the exclusive control of the Holder (see section 6.2.8 above).

6.2.10 Method of destroying private keys

6.2.10.1 CA private key

The destruction of CA private keys can only be carried out following an end of life ceremony with the presence of qualified personnel and the secret bearers.

At the end of the life of a CA private key, normal or anticipated (revocation), this key is systematically destroyed, along with any copy and any element allowing it to be reconstituted.

6.2.10.2 Holder's private key

The destruction of the Holder's private keys is automatically carried out following the revocation or expiration of the key.

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

6.2.11.1 Cryptographic module used for the private keys of the CA

The cryptographic module used by the CA meets the following certification requirements:

- EAL 4+ to the Common Criteria ISO / IEC 15408 (conforms to the Protection Profile CWA 14167-2 or CWA 14167-3); or

- FIPS 140-2 level 3
- or equivalent.

6.2.11.2 Cryptographic module used for the private keys of the Holders

NG Technologies does not provide a signature creation device to Holders. The Holders' signature creation systems remain under the control of NG Technologies. These devices must meet at least the following certifications:

- FIPS 140-2 level 3
- or equivalent.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

Public keys are archived in X.509 certificate format in DER encoding (see section 5.5).

6.3.2 Lifespans of key pairs and Certificates

- The lifespan of CA certificates: 20 years
- The lifetime of the Time Stamping Authority certificate: 5 years
- The life of the Holders' certificates: 1 day to 2 years.

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

The CA key activation data is generated during the key ceremony. These activation data are stored on smart cards and given to secret carriers.

Each bearer of secrets takes the necessary measures to protect themselves against the loss, theft, unauthorized use or unauthorized destruction of their smart card and the activation data it contains.

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

See Section 6.2.8.2.

6.4.2 Activation data protection

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

The activation data is stored on a nominative and personal card.

Responsibility for this smart card rests with the person to whom the card is issued. The card is protected by a personal password with the bearer of the secret. The smart cards are then stored in an individual secure safe.

Each secret bearer is responsible for his share of the activation secret. He expresses his consent by signing a form defining his responsibilities.

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

Each Holder must take the necessary measures to protect themselves against the loss, theft and unauthorized use of their authentication secrets. He is solely responsible for protecting these secrets.

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

All machines (servers and client workstations) that are part of or can connect to NGRTS components are protected by access control. The logs are regularly checked. Users do not have root access and cannot install software unless approved by CISO who alone has root access.

Any access to the cryptographic module holding the keys requires the physical presence of at least two NG Technologies employees with trusted roles.

Additional access control and authentication mechanisms are in place for all roles allowing the generation of new certificates.

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

The software used by the various technical components of NGRTS has been implemented with respect for good practices in terms of safety, quality and performance.

The software is documented. Any update is documented and traced (subject, date and author of the modifications). A modification is only pushed into production following a well-defined and documented quality process including a code review and acceptance test phase.

6.6.2 Safety management measures

See section 6.6.1 above.

6.6.3 Systems lifecycle security assessment level

Not applicable.

6.7 Network security measures

The software used by the various technical components of NGRTS is hosted in physical private hosting in a Datacenter. The Datacenter is certified Tier 4.

Remote access is only possible for externally exposed web services. All administration services require two factor authentification.

All the services are protected by "firewall" type gateways segmenting the networks according to their sensitivity. These gateways are configured to only accept flows that are strictly necessary.

6.8 Timestamp / Dating system

To date the events, the various technical components of NGRTS have recourse to the system time of by ensuring a synchronization of the clocks of the systems between them, at least to the minute, and with respect to a reliable source of UTC time.

The time used for the provision of system date is be synchronized with UTC at least once every 24 hours.

7 PROFILE OF CERTIFICATES, OCSPS AND CRLS

7.1 Certificate Profile

All Certificates issued by NGRTS comply with X.509 v3 format.

Certificates contain the following primary fields and extensions.

7.1.1 Certificate of the Intermediate Certification Authority RT CA

Basic fields

Field	**Value**
Version	X.509 version 3
Serial number	236625553420133709196276053786618712628947920708
Signature Algorithm (OID compliant with RFC 5280)	RSA / Sign, hash = SHA-256, padding = 1.5, length = 4096
Issuer	CN = NG Technologies Root CA, O = NG Technologies, OU = NG PKI, C = TN
Subject	CN = NG Technologies RT CA, O = NG Technologies, OU = NG PKI, C = TN
Validity	20 years

Extensions

Field	**Critical**	**Value**
Authority Key Identifier	No	4DF2C7882770E188BD099317D8E13D2785C72403
Subject Key Identifier	No	8702F9CC1404B034FA1EA22E874158AEC838CB1A
Key Usage	Yes	keyCertSign, CRLSign
Basic Constraint	Yes	• Certificate Authority: yes • Maximum Path Length: 0
CRL Distribution Points	No	Download URL of the latest CRL issued by the Root CA. https://pki.ng-cert.com/repository/public/ng-root-ca-lar.crl
Authority Info Access	No	If present, contains the URL of the Root Certificate CA : https://pki.ng-cert.com/repository/public/root.crt
Certificate Policies	No	• Policy OID: 2.16.788.2.1.2 • cPSuri: policy download link https://www.ng-cert.com/repository/public/

7.1.2 Holders Certificates

Basic fields

Field	**Value**

Version	X.509 version 3
Issuer DN	The DN of this AC defined above.
Subject DN	The DN of the Holder in accordance with section 3.1.1
Serial number	Numeric value. Serial numbers for issued certificates are never used twice.
Signature Algorithm (OID compliant with RFC 5280)	RSA / Sign, hash = SHA-256, padding = 1.5, length = 2048

Extensions

Field	**Critical**	**Comment**
Authority Key Identifier	No	See 7.1.1 above.
Subject Key Identifier	No	Automatically generated when the certificate is generated in accordance with RFC 5280.
Key Usage	Yes	digitalSignature, nonRepudiation
Extended Key Usage	No	clientAuth, emailProtection
Basic Constraint	No	Certificate Authority: no
CRL Distribution Points	No	Download URL of the latest CRL https://pki.ng-cert.com/repository/public/ng-rt-ca.crl
Authority Info Access	No	If present, contains the URL of the OCSP server.
Certificate Policies	No	• Policy OID: 2.16.788.2.1.2 • cPSuri: policy download link (https://www.ng-cert.com/repository/public/)
Alternative subscriber name (subjectAltName)	No	Holder email.
QCStatements	No	• Qualified Certificate: Yes • Private Key in SSCD: Yes • QC type: id-etsi-qct-esign

7.2 CRL Profile

Basic fields

Field	**Value**
Version	2
Signature algorithm	RSA / Sign, hash = SHA-256
Issuer DN	The DN of the CA
This Update	Date of signature of the CRL
Next Update	7 days maximum after the This Update date

Revoked Certificates (Entries)	Serial number list of revoked certificates with reason and revocation dates

Extensions

Field	Critical?	Comment
Authority Key Identifier	No	The identifier value in 7.1.1 above.
CRL Number	No	Monotonically increasing sequence number.
ExpiredCertsOnCRL	No	Date since which expired certificates are not removed from the CRL. Expired certificates are never removed since the first issued CRL.

7.3 OCSP Profile

7.3.1 Basic fields

Field	Value
Version	1
Response Type	Basic OCSP Response
Issuer DN	The DN of the CA
Produced At	Date of the production of the OCSP
This Update	Date of signature of the OCSP
Next Update	7 days maximum after the This Update date
Signature Algorithm	sha256WithRSAEncryption

7.3.2 Extensions

Field	Critical?	Comment
Nonce	No	Nonce to be used in the response.
Extended Revoked	No	Extension as defined in RFC 6960

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.

NG Technologies is certified EU Regulation 910/2014 (eIDAS), ETSI EN 319 401, ETSI EN 319 411-1 & 2 and ETSI EN 319 412-2 & 5.

Regular (biannual) audits are carried out by European cabinet accredited in accordance with the ISO/IEC 17065:2012 Standard and ETSI EN 319 403-1 V2.3.1.

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 RT 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.

8.6 Communication of results

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

9 OTHER COMMERCIAL AND LEGAL ISSUES

9.1 Prices

The prices for the services offered by NG Technologies are published on the NG Technologies website.

9.1.1 Prices for access to Certificates

Access to CA certificates is free and public.

Access to clients' certificates is possible free by web services but need to be authorized.

9.1.2 Tariffs for accessing certificate status and revocation information

Downloading CRLs is free.

Access to the OCSP service is free.

9.1.3 Prices for other services

NG Technologies can add other optional paid services. The conditions and prices will be published on the NG Technologies website.

9.1.4 Refund policy

The services are not subject to any reimbursement.

9.2 Financial responsibility

9.2.1 Insurance coverage

NG Technologies maintains appropriate liability insurance allowing to cover the financial risks associated with the use of the services it is providing.

9.2.2 Other resources

NG Technologies maintains an updated business models and a financial policy aimed at maintaining throughout its activity the financial resources necessary to fulfill the obligations defined by the CP.

9.2.3 Coverage and guarantee for user entities

No Stipulation.

9.3 Confidentiality of professional data

9.3.1 Scope of confidential information

The following information is considered confidential:

- The private keys of the CA,
- Activation data associated with private keys
- Event logs
- Supporting documents for registration files,

Depending on the context, other information may be considered confidential and treated as such.

9.3.2 Information outside the scope of confidential information

Not applicable.

9.3.3 Responsibilities in terms of protecting confidential information

NG Technologies undertakes to treat confidential information managed by the components of NGRTS in accordance with the obligations applicable to it.

9.4 Protection of personal data

9.4.1 Personal data protection policy

NG Technologies respects the laws and regulations in force for the management and use of personal data.

9.4.2 Personal information

Personal information is the personal information of the holder, recorded in the Certificate Holder file. This is the name / first name / address / telephone / function / email information. Personal information included in the signing certificate is not considered confidential (see section 7 for the certificate profile). This information is public (because the certificates are public) and the Holder declares his acceptance of the publication of this information upon acceptance of the usage terms.

9.4.3 Non-personal information

Not applicable.

9.4.4 Responsibility in terms of personal data protection

NG Technologies is responsible for the protection of personal data processed by the technical components of NGRTS.

9.4.5 Notification and consent to use personal data

The certificate holder is informed of the use made by NG Technologies of this personal data, during the acceptance phase of the conditions of use when doing the certificate request.

9.4.6 Conditions of disclosure of personal information to judicial or administrative authorities

Personal information may be made available to judicial or administrative authorities under the conditions provided for by regulations in Tunisia.

9.4.7 Other circumstances of disclosure of personal information

Not applicable.

9.5 Intellectual and industrial property rights

When performing the services defined in this document and / or any other contractual document relating to a service offered by NG Technologies through its NGRTS platform, it may be delivered elements protected by copyright.

These elements, as well as the copyrights attached to them, will remain the property of the holder of the corresponding rights.

9.6 Contractual interpretations and guarantees

9.6.1 Certification Authority

The CA is responsible for:

- the protection (integrity and confidentiality) of the private key during generation and throughout the
validity of the key as well as the activation data;
- the use of key pairs and certificates for which they were issued, in accordance with the applications defined in this CP;
- publication of the public information related to the operation of the CA, in a sustainable and secure way;
- submitting to compliance checks carried out by external or internal auditors and implementing work of their recommendations;
- proper documentation of internal operating and use procedures;
- sensitizing staff to trust their commitments.

The CA is responsible for the damages caused to the User Parties if:

- The information contained in the Certificate does not correspond to the information contained in the registration request;
- The CA has not revoked a Certificate and / or has not published this information under the conditions provided for by the CP.

9.6.2 Certificate holder

The holder:

- Must provide accurate and up-to-date information when requesting the establishment of a Certificate;
- Is responsible for access to his private key and, where applicable, the means of activating his key;
- Must respect the conditions of use of his private key;
- Must inform the CA of any modification of the information contained in its Certificate;
- Must send a request for revocation of his Certificate without delay in the event of suspicion of compromise of the corresponding private key or of the means of activating this key.

9.6.3 User Parties

The User Parties undertake to comply with the obligations provided for in the User Agreement and to be aware of the terms and conditions of the CP applicable to the service they are using, in particular the limits of use and guarantees associated with the service.

9.6.4 Other participants

Not applicable.

9.7 Warranty limit

The CA's warranty limits are provided for in the General Conditions of Use of NG Technologies services.

9.8 Limitation of Liability

- The CA is not responsible for any use of Certificates that is unauthorized or does not comply with the CP, the Subscription Agreement or the User Agreement.
- The CA cannot be held responsible for indirect damages linked to the use of a Certificate.
- The CA is not responsible for the use of the private keys associated with the Certificates or the activation data of these keys.
- The CA is not responsible for the unauthorized or non-compliant use of the equipment and / or software made available to users of the certification service.
- The CA declines all responsibility in the event of damage resulting from errors or inaccuracies in the information contained in the Certificates, when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the Holder.

9.9 Indemnities

Not applicable.

9.10 Duration and early termination

9.10.1 Period of validity

This document is applicable from the date of publication of the CP until the end of life of the last certificate issued under this CP.

9.10.2 Early end of validity

The CP remains in force until it is replaced by a new version.

9.10.3 Effects of the end of validity and remaining applicable clauses

Not applicable.

9.11 Individual notifications and communications between participants

All individual notifications and communications provided for by the CP must be sent by means guaranteeing their origin and receipt.

9.12 Amendments

9.12.1 Amendment procedures

NG Technologies can amend the PC. These amendments take the form of new versions of the PC.

They are published on the NG Technologies publication site. NG Technologies determines if the modifications to the PC require a change of the OIDs for the issued Certificates.

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.

9.12.2 Mechanism and information period on amendments

NG Technologies can make changes without notifications on the current PC in the event of a minor change, such as typographical or URL corrections.

NG Technologies is the only entity authorized to assess whether a modification is minor.

9.12.3 Circumstances under which the OID must be changed

In the event of a substantial modification of the PC, NG Technologies may decide that a change of OID is necessary.

9.13 Dispute Resolution Provisions

In the event of a dispute between NG Technologies and a user of its services, amicable voice is the first recourse. In the event of failure, the parties have recourse to the common law jurisdiction, knowing that NG Technologies attributes jurisdiction to the Court of Tunis.

9.14 Competent courts

See above.

9.15 Compliance with laws and regulations

The provisions of the PC comply with the requirements of European Law (eIDAS) and Tunisian Law.

See paragraph Compliance audit and other assessments.

9.16 Miscellaneous

9.16.1 Global agreement

Not applicable.

9.16.2 Transfer of activities

Not applicable.

9.16.3 Consequences of an invalid clause

Not applicable.

9.16.4 Application and waiver

Not applicable.

9.16.5 Force majeure

Are considered as force majeure all those usually retained by Tunisian law in particular the case of an irresistible, insurmountable, and unforeseeable event.

9.17 Other provisions

Not applicable.