PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

NATIONAL ELECTRONIC CERTIFICATION AUTHORITY

Algeria National PKI Framework

National Root Certification Authority CP/CPS

Version 2.2

Document Management

Information

Group of document	Algeria National PKI Framework
Title	National Root Certification Authority CP/CPS
Status	**Released**
Project reference:	Algeria National PKI
Annex:	n.a.

Version History

Version	Date	Description / Status	Responsible
V0.1	15/01/2019	Initial document preparation	ANCE (PMA)
V0.2	30/02/2019	Amendments after customer agreements on PMA governance structure	ANCE (PMA)
V0.3	27/04/2019	Complete first draft after final CPS workshops	ANCE (PMA)
V0.4	30/09/2019	Typos + key lifetimes change and feedback from customer.	ANCE (PMA)
V0.5	25/10/2019	Additional feedback from customer	ANCE (PMA)
V0.6	08/12/2019	Additional feedback from customer. Version ready for final review and sign off	ANCE (PMA)
V0.7	29/01/2020	Amendments to accommodate auditor feedback	ANCE (PMA)
V1.0	20/03/2020	Changing CA DNs and URLs as per final decisions from PKI management	ANCE (PMA)
V1.1	25/10/2020	Applying final comments from the WebTrust Auditor	ANCE (PMA)
V1.2	01/10/2021	Yearly review	ANCE (PMA)
V2.0	01/06/2022	• Certificate profiles updated following the new Baseline requirements related to adding Extended Key Usage (EKU) extensions to all Subordinate CAs certificates under the National Root CA. • Reflect the new PKI Hierarchy of Government Domain • Alignment to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.8.0 which is linked to WebTrust for SSL BR v2.6 • Alignment to Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates v2.7 which is linked to WebTrust for CS BR v2.7	ANCE (PMA)

V2.1	18/06/2023	Yearly review • With changes In the Algerian national PKI hierarchy schema to reflect the current hierarchy of the governmental domain • Certificate profiles updated following the new Baseline Requirements for the issuance and management of Publicly-Trusted Certificates v2.0.0	ANCE (PMA)
V2.2	10/10/2023	• Major changes following the new Baseline requirements related to Extended Key Usage (EKU) that constraints all Subordinate CAs under the National Root CA. • Update the Algerian national PKI hierarchy schema to reflect the current hierarchy of the commercial PKI domain • New Algerian National PKI Hierarchy description • Review/update certificate profiles of AECE following the new Baseline requirements related to adding Extended Key Usage (EKU) extension.	ANCE (PMA)

Document Signoff

Version	Date	Responsible	Validated By	Publication Approved By
V2.2	24/10/2023	ANCE (PMA)	ANCE (PMA) 24/10/23	ANCE (PMA) 24/10/23

Table of contents

1 Introduction

The present Certificate Policy and Certification Practice Statement (hereinafter, CP/CPS) of the National Root Certification Authority (hereinafter, NR-CA) of Algeria applies to the root-signing services of the NR-CA. It also applies to the PKI domains established under the NR-CA and relevant relying parties.

This CP/CPS adopts international, WebTrust and CA/Browser Forum Guidelines targeted at trustworthy systems dealing with publicly trusted PKI certification services.

This CP/CPS complies with the formal requirements of Internet Engineering Task Force (IETF) [RFC 3647] with regard to format and content. While certain clause titles are included according to the structure of [RFC 3647], the topic may not necessarily apply in the implementation of the PKI services of the National Root CA. Such clauses are denoted as “not applicable”.

The CP/CPS complies with the Algerian Law No. 15-04 meant to regulate digital certification services in Algeria. Moreover, it defers to existing and internationally recognized standards, and references clauses from these standards, wherever it is relevant.

The CP/CPS addresses the technical, procedural and organisational policies and practices of the NR-CA with regard to all services available during the lifetime of certificates issued by the NR-CA.

The CP/CPS is public. Wherever confidential information is referenced herein, the text refers to classified documentation that is available to authorised persons only.

Further information with regard to this CP/CPS and the NR-CA can be obtained from the Policy Management Authority (PMA), using contact information provided in clause 1.5.

1.1 Overview

The Algeria National PKI is implemented as two separate PKI domains (Government and Commercial) established under the Algeria NR-CA. With this National PKI, the Algerian Government aims to provide a framework to facilitate the establishment of Trust Service Providers (TSP) offering digital certification and trust services to government and non-government entities.

The Algeria PKI hierarchy comprises a hierarchy of Certification Authorities (CAs).

The NR-CA sits at the top level of the hierarchy and acts as the trust point (anchor) for the Algerian PKI. The National Authority for Electronic Certification (Autorité Nationale de Certification Electronique – ANCE) is established by the Algerian government to operate the NR-CA. The ANCE as the national PKI governance body, is responsiblefor operating the Policy Management Authority (PMA).

The Government Authority for Electronic Certification (Autorité Gouvernementale de Certification Electronique – AGCE) is established by the Algerian Government to operate the Government CAs (GOV-CAs) and to offer related trust services to the Algerian government domain. As such the AGCE operates as a Trust Services Provider (TSP) offering its services through a hierarchy of CAs, implemented under the National Root CA as follows:

- **Government CAs:** five (05) Intermediate GOV-CAs certified by the Root CA: Government CA, Government TLS CA, Government CS CA, Government SMIME CA and Government TS CA.

  Each GOV-CA certifies one issuing CA to cover particular Extended Key Usages as follows:

  - **Corporate CA:** Issuing CA under Government CA that will issue Digital Signature and Authentication certificates to natural persons (government employees) and legal persons (government entities).

- **OV TLS CA:** Issuing CA under Government TLS CA that will issue organization validated Server Authentication certificates to non-natural entities such as web servers and VPN device certificates. It will also issue Client Authentication certificates to organization's devices.
- **SMIME CA:** Issuing CA under Government SMIME CA that will issue email protection (S/MIME) certificates to natural persons (government employees).
- **Code Signing CA:** Issuing CA under Government CS CA that will issue code signing certificates to legal persons (government entities).
- **Trust services CA:** Issuing CA under Government TS CA that will issue timestamping certificates for AGCE and Government TSPs operating Timestamping service. It will also issue signing certificates to governmental TSPs operating Digital Signature Verification Service to digitally sign verification responses.

In addition to the above issuing CAs, there is a scenario where a Governmental TSPs can establish their own

certification services under the Government CA. The GOV-CA will certify an issuing CA operated by the TSP.This CA shall be technically constrained where the CA certificate (issued by the GOV-CA) will be populated with a combination of extended key usage and name constraint extensions to limit the scope within which the issuing CA from the TSP may issue end-user certificates.

The AGCE is responsible for the supervision and authorization of the TSP that shall successfully complete an authorisation process.

The governance structure of the AGCE PKI is referred to as the AGCE PKI Governance Board (AGCE PKI GB). The PKI GB is composed of senior consultants appointed from PKI unit within AGCE, it is responsible for maintaining CP and CPS documents relating to certificates within AGCE PKI. It interacts closely with the PMA to implement the GOV-CA operational cycle.

The Algerian Government tasked the Post and Electronic Communication Regulation Authority (Autorité de Régulation de la Poste et des Communications Électroniques - ARPCE) to oversee the establishment of TSPs and to offer related trust services under the Economic PKI branch. In this context, the ARPCE operates as the Economic Authority for Electronic Certification (Autorité Economique de Certification Electronique – AECE). The AECE implements and operates two (02) intermediate Commercial CAs which known as COM-CA.certified by the National Root CA to cover particular extended Key usages implemented by AECE as follows:

Commercial CAs:

Two (02) Intermediate CAs (Technically constrained subordinate CAs) certified by the National Root CA, namely: **Commercial CA** and **Commercial TS CA**.

- **Commercial CA :** Subordinate CA Technically constrained certified by National Root CA
  - **AECE Signing CA :** Subordinate CA Technically constrained certified by the **Commercial CA,** that will issue certificates to natural persons and legal persons for authentication and electronic signature,
- **Commercial TS CA:** Subordinate CA Technically constrained certified by National Root CA , that **Certify the issuing CAs under the economic branch to cover TimeStamping extended key usage.**

In addition,the overall mandate of the AECE is to authorize and supervise the operations of organizations offering certification and trust services to be certified by the COM-CA. to establish certification services for TSPs.The COM-CA will certify an issuing CA operated by the TSP. In this case the CA shall be technically constrained where the CA certificate will be populated with a combination of extended key usage and name constraint extensions to limit the scope within which the issuing CA from the TSP may issue end-user certificates.

The AECE is responsible for the supervision and authorization of the TSP that shall successfully complete an authorization process.

The governance structure of the AECE PKI is referred to as the AECE PKI Governance Board (AECE PKI GB). The PKI GB is composed of senior consultants appointed from PKI unit within AECE; it is responsible for maintaining this and other CP and CPS documents relating to certificates within AECE PKI. It interacts closely with the PMA to implement the COM-CA operational cycle.
The abbreviations ARPCE and AECE will be used interchangeably hereinafter.

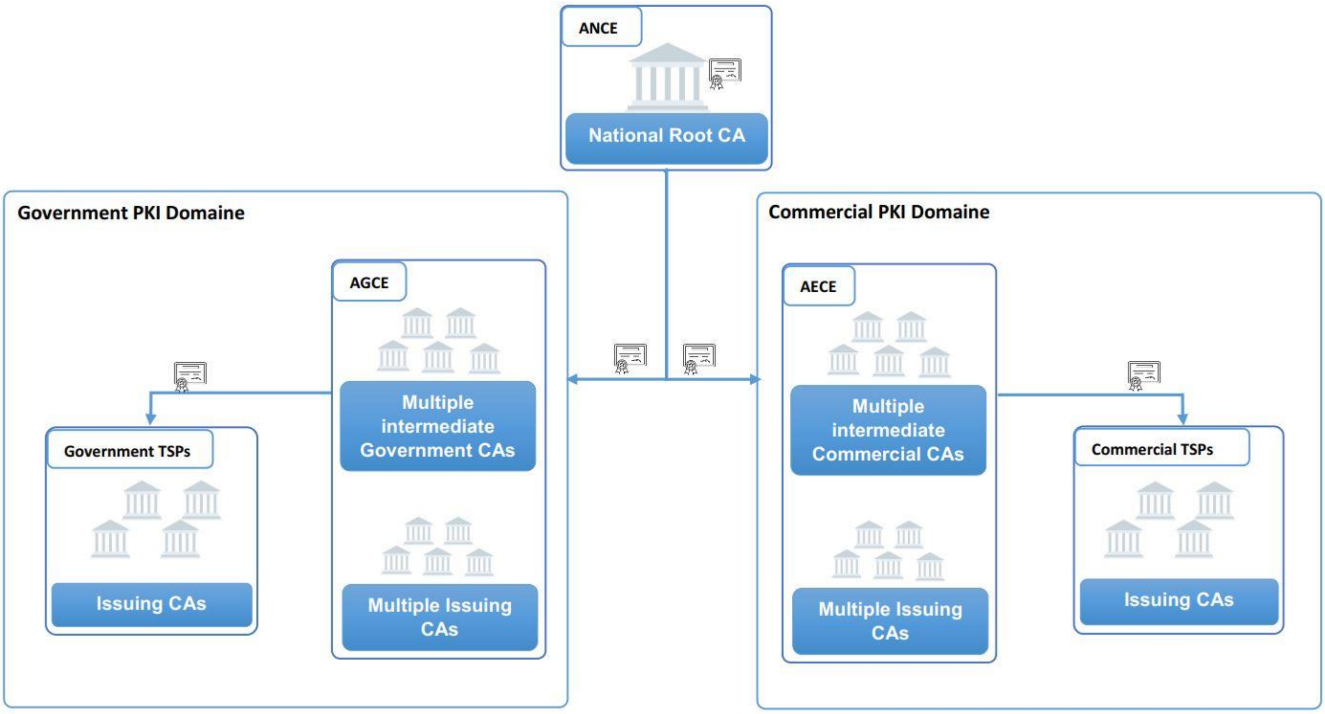

Figure 1: The Algerian National PKI hierarchy

1.1.1 Overview of the PMA role

The ANCE acts as the governance body for PKI in Algeria. Its operations are established as part of the initial Go-live of the NR-CA. Representatives from the ANCE, the AGCE and the AECE constitute the organisational structure of the PMA.

The mandate of the PMA is summarized as follows:

1. **Responsible for NR-CA operations:** The PMA operates the Registration Authority (RA) function of the NR-CA. The PMA delegated the technical operations of the NR-CA to the AGCE. A PMA meeting organized before the initial NR-CA key ceremony acknowledged the PMA decision to delegate the operations of the NR-CA to the AGCE;
2. **Develop the national PKI framework:** This framework includes CP and CPS documentation, governance framework, security policies and related documentation used to oversee the establishment of TSPs and the rollout of certification and trust services in Algeria;
3. **Oversees the AECE operations:** The PMA approves the AECE in its role of the authority in charge of supervising TSPs under the Commercial PKI domain. As such, the PMA authorizes the establishment of the Commercial CAs under the custody of the AECE. The PMA oversees the operations of the Commercial CAs through regular interactions with the Commercial CAs management Board;
4. **Oversees the AGCE operations:** The PMA approves the AGCE as a TSP offering certification services to government entities. As such, the PMA authorizes the establishment of the Government CAs and related trust services operated by the AGCE. The PMA oversees the operations of the AGCE TSP operations through regular interactions with the Government CA management Board**;**
5. **Managing the international recognition of the Algerian Root CA:** This will be organized through a WebTrust certification program of the Root CA certificate covering the Commercial and Government CAs. It also includes inclusion into vendor programs and CA/Browser forum;
6. **Manage the country's Trust List:** The PMA will manage the list of approved TSPs under the Government and Commercial PKI domains**.**

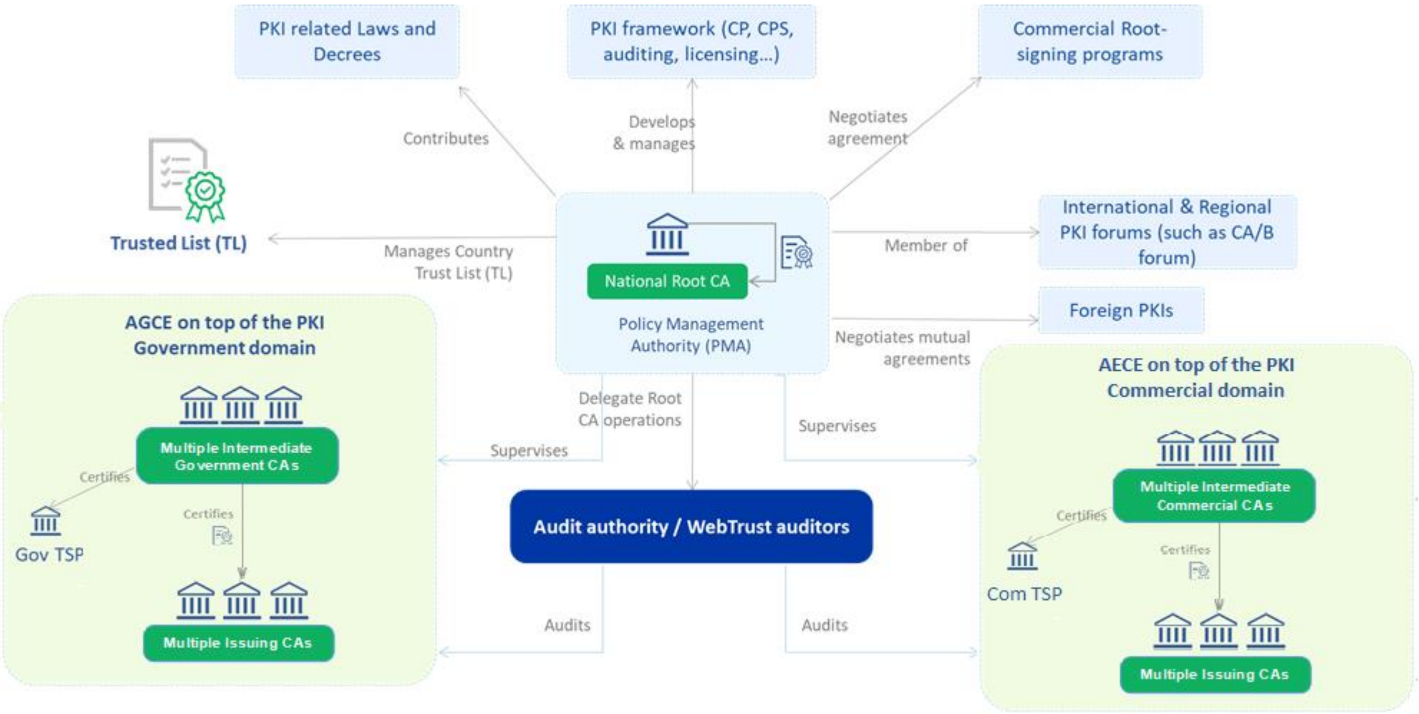
PKI related Laws and Decrees
PKI framework (CP, CPS, auditing, licensing...)
Commercial Root-signing programs
Contributes
Develops & manages
Negotiates agreement
Trusted List (TL)
Manages Country Trust List (TL)
National Root CA
Policy Management Authority (PMA)
Member of
International & Regional PKI forums (such as CA/B forum)
Foreign PKIs
Negotiates mutual agreements
AGCE on top of the PKI Government domain
Multiple Intermediate Government CAs
Certifies
Gov TSP
Certifies
Multiple Issuing CAs
Delegate Root CA operations
Supervises
Supervises
Audit authority / WebTrust auditors
Audits
Audits
AECE on top of the PKI Commercial domain
Multiple Intermediate Commercial CAs
Certifies
Com TSP
Certifies
Multiple Issuing CAs

Figure 2: The Algerian National PKI framework hierarchy

1.2 Document Name and Identification

This document is named “**Algeria Root CA CP/CPS**” and is referenced in related documents.

The NR-CA will use the **OID 2.16.12.3.1.1.1** to identify this document.

1.3 PKI Participants

Several parties constitute the participants of this NR-CA PKI. The parties mentioned hereunder including the NR-CA, NR-CA RA, PMA, subscribers and relying parties are collectively called PKI participants.

1.3.1 Certification Authorities

The NR-CA is the Certification Authority that issues Certificates in accordance with this CP/CPS under the responsibility of the PMA. The NR-CA is technically operated by the AGCE as per the delegation from the PMA to the AGCE. However, the PMA assumes the RA role for the NR-CA.

Pursuant to the broad and public purpose of digital certificates, the PMA seeks for inclusion and maintenance of the NR-CA into major operating system and software providers (namely into the corresponding “root programs” from Google, Apple, Microsoft, Adobe and Mozilla). This will result in the recognition of the NR-CA certificate in off-the-shelf applications and web browsers, supporting the technical and trust recognition of the electronic signatures, electronic end-entity certificates and other trust service outputs from the TSP services approved under the Algerian PKI framework.

1.3.2 Registration Authorities

The PMA operates a single RA for the NR-CA. This RA is tasked to request the issuance and the revocation of certificates under this CP/CPS from the AGCE operating the NR-CA. The PMA organizational structure includes the Registration Authority Officer (RAO). The RAO is responsible for the execution of the NR-CA operational cycle, including the key ceremonies for the Government and Commercial CAs, as well as the generation of Certificate Revocation Lists (CRL).

1.3.3 Subscribers

The subscribers are:

Government CA, Government TLS CA, Government CS CA, Government SMIME CA, Government TS CA;

the Commercial CA and the Commercial TS CA. These CAs are collectively called “Subscribing CAs or

Subordinate CAs”.

These subscribers:

- are identified in the Subject field of their certificate, issued by the NR-CA;
- control the private key corresponding to the public key that is listed in their certificate.

1.3.4 Relying Parties

Relying parties are natural or legal person entities who rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber’s certificate.

To verify the validity of a digital certificate issued by the NR-CA, relying parties must always verify the certificate status against the NR-CA certificate validity status service (e.g. OCSP).

1.3.5 Other participants

There are no other participants for this CA.

1.4 Certificate Usage

The following limitations hereunder apply to the usage of certificates issued by the NR-CA.

1.4.1 Appropriate certificate uses

The NR-CA root (self-signed) certificate can be used to:

- Sign certificates for the Government CAs and the Commercial CA;
- Sign CRLs containing the list of subscribers’ revoked certificates and of NR-CA revoked self-signed certificates;
- Sign OCSP certificates for the NR-CA OCSP service.

The Government CAs certificates can only be used to:

- Sign certificates for issuing CAs operated by the AGCE;
- Sign certificates for issuing CAs operated by TSPs that are authorized by the PMA to offer certification services under the PKI Government domain;
- Sign CRLs, containing the list of Government CAs subscribers’ revoked certificates;
- Sign OCSP certificates for the Government CAs OCSP service.

The Commercial CA certificates can only be used to:

- Sign certificates for issuing CAs operated by TSPs that are licensed by the AECE to offer certification services under the PKI Commercial domain;
- Sign CRLs containing the list of Commercial CA subscribers' revoked certificates;
- Sign OCSP certificates for the Commercial CA OCSP service.

1.4.2 Prohibited certificate uses

The NR-CA cannot be used to sign end-entity certificates (other than the certificate of its OCSP server).

The Government CAs and Commercial CA are not authorized to issue end entity certificates (other than certificates for their respective OCSP services) or to offer services that fall out of the scope of what is described in their CPS.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The PMA has the overall responsibility for producing and publishing this document. The PMA is also responsible for maintaining the PKI OID sub-tree used to provide OID values for the different documents produced in the context of the Algerian PKI framework.

The PMA is comprised of members with relevant PKI policy experience and appointed to conduct the following tasks in relation to the PKI policy administration:

- Approve the AGCE and the AECE operational practices and policies in relation to their respective roles of operators of the Government CAs and Commercial CA;
- Support the supervisory process on the NR-CA operations by the AGCE team in accordance with the practices of the CP/CPS. In addition, supervise the AGCE and the AECE operations;
- Produce, maintain, and publish the relevant policy documentation for the Algeria PKI framework;
- Produce the key ceremony documentation for the NR-CA;
- Assess the changes required to the PKI design and reflect these changes on the related NR-CA policy documentation.

1.5.2 Contact person

The PMA can be contacted at the following address:

Policy Management Authority
Autorité Nationale de Certification Electronique.
Cyber Park Sidi Abdellah, Bt D,
Rahmania, Zeralda,
Alger.
Tel: + 213 (0) 23 202 327
Fax: + 213 (0) 23 202 327
Email: ANCE.Certification.Info@agce.dz

The PMA accepts comments regarding the present CP/CPS only when they are addressed to the contact above.

Certificate Problem Report

Subscribers, relying parties, application software suppliers, and other third parties can report suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to any certificates issued under the NR-CA by sending an email to ANCE.Certification.Problem@agce.dz.

The PMA will validate and investigate the request before taking an action in accordance to section 4.9.

1.5.3 Person Determining CPS Suitability for the Policy

The PMA bears responsibility for the drafting, publishing, maintaining, and interpreting of this CP/CPS.

1.5.4 CPS approval procedures

A dedicated process involves the PMA reviewing the initial version of this CP/CPS and any subsequent updates. Amendments are in the form of a document containing an amended form of the CP/CPS or an update notice.

1.6 Definitions and Acronyms

1.6.1 Definitions

The following is a list of the definitions of terms and acronyms used in this CP/CPS. The source is cited where relevant.

Applicant — The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. In the context of this CP/CPS, AGCE and AECE are the applicants represented by their PKI GB.

Applicant Representative — A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA. In the context of this CP/CPS, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant.

Activation data — Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected; e.g. a PIN, a password or pass-phrase, or a manually held key share.

Attestation Letter — A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information. In the context of this CP/CPS, attestation letters are signed by Human Resource teams of government entities.

Audit Period — In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA)

CA Key Pair — A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate — An electronic document that uses a digital signature to bind a public key and an identity

Certificate Policy (CP) — A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report — Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List — A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority — An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement — One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Profile — A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Control — "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country — Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

CSPRNG — A random number generator intended for use in cryptographic system.

Expiry Date — The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

HSM — Hardware Security Module — a device designed to provide cryptographic functions specific to the safekeeping of private keys

IP Address — A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

Issuing CA — In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA. In the context of this CP/CPS, the National Root CA is an issuing CA.

Key Compromise — A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script — A documented plan of procedures for the generation of a CA Key Pair.

Key Pair — The Private Key and its associated Public Key.

Legal Entity — An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier — A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder — An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol — An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key — The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key — The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure — A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate — A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor — A natural person or Legal Entity that meets the requirements of Section 8.2.

Registration Authority (RA) — Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA. The PMA operates the RA for the National Root CA.

Relying Party — Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository — An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA — The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate — The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject — The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information — Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA — A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber — A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement — An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subscribing CA — In the context of this CP/CPS, Subscribing CAs are AGCE Government CAs and AECE Commercial CAs whose certificates are signed by the Algeria National Root CA.

Terms of Use — Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Valid Certificate — A Certificate that passes the validation procedure specified in RFC 5280.

Validity Period — The period of time measured from the date when the Certificate is issued until the Expiry Date.

1.6.2 Acronyms

AECE	Autorité Économique de Certification Électronique AGCE
	Autorité Gouvernementale de Certification Électronique
AICPA	American Institute of Certified Public Accountants
ANCE	Autorité Nationale de Certification Électronique
ARPCE	Autorité de Régulation de la Poste et des Communications Électroniques
CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
COM-CA	Commercial CA
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Curriculum Vitae
DN	Distinguished Name
FIPS	Federal Information Processing Standards
GOV-CA	Government Certification Authority
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Standards Organization
NR-CA	National Root CA
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Information Number
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PKI GB	PKI Governance Board
PMA	Policy Management Authority
PSCE	Prestataire de Service de Certification Électronique
RA	Registration Authority
RSA	Rivest-Shamir-Adelman (The names of the inventors of the RSA algorithm)
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TC	Tiers de Confiance
TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider (collective term for TCs and PSCE

UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator
VPN	Virtual Private Network

1.6.3 References

This document refers to the following:

- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- AICPA/CPA Canada WebTrust For Certification Authorities Principles And Criteria
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- AICPA/CPA Canada WebTrust Principles And Criteria For Certification Authorities – Code Signing Baseline Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates
- CA/B Forum Network and Certificate System Security Requirements
- Algerian Law 15-04 on « *Digital Signature and Electronic certification* » (*Loi n° 15-04 du 01 Février 2015, fixant les règles générales relatives à la signature et à la certification électroniques*
- Executive Decree No. 16-134 of ANCE
- Executive Decree No. 16-135 of the AGCE

2 Publication and Repository Responsibilities

2.1 Repositories

The NR-CA operations team publishes information about NR-CA certificates, CRLs for issued certificates, CP/CPS documents and agreements in a public repository that is available 24 × 7 and accessible at https://ca.pki.ance.dz/repository.

2.2 Publication of Certification Information

As part of the online repository, the NR-CA operations team maintains documents making certain disclosures about the NR-CA practices, procedures and the content of some of its policies, including this CP/CPS. The PMA will at all times make available the current versions of the NR-CA CP/CPS document on its public repository.

The online repository is available 24 × 7 and accessible at https://ca.pki.ance.dz/repository.

The PMA reserves its right to make available and publish information on the NR-CA practices, as it sees fit.

The NR-CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those requirements, the requirements take precedence over this document.

The NR-CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those requirements, the requirements take precedence over this document.

With regard to the NR-CA activities, and due to their sensitivity, the NR-CA operations team refrains from making publicly available certain subcomponents and elements of certain documents. However, such documents and documented practices are conditionally available to designated authorised parties in the context of audit(s).

The NR-CA publishes digital certificate status information in intervals indicated in this CP/CPS. The provision of NR-CA issued electronic certificate validity status information is a 24x7x365 service.

- The NR-CA publishes CRLs including any changes since the publication of the previous CRL, at regular intervals.
- The NR-CA maintains an OCSP responder compliant with RFC 6960. OCSP information is available immediately to relying party applications. The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by the NR-CA.

The NR-CA operations team maintains the Certificate Dissemination webpage, the CRL distribution point and the information therein, the OCSP responder and the information therein, as long as there are non-expired certificates containing the CRL distribution point.

2.3 Time or Frequency of Publication

The NR-CA and OCSP certificates are published to the NR-CA public repository once they are issued.

A CRL is issued by the NR-CA every six months. In addition, a new CRL will be generated and published following the revocation or issuance of any certificate.

The NR-CA operations team ensures that the CP/CPS of NR-CA is reviewed at least once annually and makes appropriate changes so that the NR-CA operations remain fully aligned to the CA/B forum Baseline Requirements and other requirements as listed in the “References” section of this CP/CPS.

Modified versions of the CP/CPS are published within seven days maximum after the PMA approval.

2.4 Access controls on repositories

Public read-only access is given to the NR-CA repository. Security controls are implemented on the repository by the NR-CA operations team to prevent any unauthorized addition, or modification of the data published on the public repository.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The NR-CA follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names.

Names have to be meaningful and unique.

The **NR-CA** self-signed certificates bear the following DN:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE

- **CommonName**: National Root CA

The **NR-CA** OCSP certificates bear the following DN:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE
- **stateOrProvinceName** : Algiers
- **CommonName**: National Root CA OCSP

The **subscribing CAs** bear the following DN:

A. The Government CA:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
- **CommonName**: Government CA

B. The Government TLS CA:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
- **CommonName**: Government TLS CA

C. The Government SMIME CA:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
- **CommonName**: Government SMIME CA

D. The Government CS CA:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
- **CommonName**: Government CS CA

E. The Government TS CA:

- **CountryName**: DZ
- **OrganizationName** : AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
- **CommonName**: Government TS CA

F. The Commercial CA:

- **CountryName** : DZ
- **OrganizationName** : AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE
- **CommonName** : Commercial CA

G. The Commercial TS CA:

- **CountryName** : DZ
- **OrganizationName** : AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE
- **CommonName** : Commercial TS CA

3.1.2 Need for Names to be Meaningful

Names are meaningful since the CN (Common Name) contains the name of the subscriber.
Subscribers cannot be anonymous or pseudonymous.

3.1.3 Anonymity or Pseudonymity of Subscribers

This CP/CPS does not permit anonymous or pseudonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in subscriber certificates are encoded according to X.500 standards and ASN.1 syntax and can be interpreted as such.

3.1.5 Uniqueness of Names

The PMA enforces the controls necessary to guarantee that subject DN are unique. Refer to section 3.1.1.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificates may be requested from the NR-CA only from the subscribing CAs and as per the naming conventions stated in this CP/CPS. Refer to section 3.1.1.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The PMA enforces validation of the proof of possession of the private key as part of the certificate request processing. The proof of possession is submitted CSRs in PKCS#10 format.

3.2.2 Authentication of Organization Identity

The identification of the subject in the certificates issued by the NR-CA will be the exact denomination of the Government CAs or the Commercial CA.

The certificates are requested by official PKI GBs representatives of the AGCE or the AECE. These official representatives must be members of the respective PKI GB, or must be duly delegated by the PKI GB. The delegation must be signed by the respective PKI GB.

A registration procedure is enforced by the NR-CA RA to perform identity verifications of the authorized representatives. This internal PMA process encompasses:

- the signature of a registration / certificate request form;
- additional paperwork provided by the respective PKI GB and used by the NR-CA RA as part of the verification process;

- review and validation by the PMA of the requesting entity CPS;
- validation of the existence of the requesting entity using the Algerian Official journal;
- site visit by a NR-CA representative to the requesting entity site in order to validate the address;
- in-person verification of the identity of the requesters against the PKI GB nominations of the related CA.

3.2.3 Authentication of Individual Identity

The NR-CA does not issue certificates for individuals.

3.2.4 Non-verified Subscriber Information

All subscriber information contained within certificate issued by the NR-CA is verified by the NR-CA RA.

3.2.5 Validation of Authority

Refer to section 3.2.2.

3.2.6 Criteria for Interoperation

No trust relationships (i.e. cross-certification) exist between the Algeria National Root and other PKI domains.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Identification and authentication for re-keying is performed as in initial registration.

3.3.2 Identification and Authentication for Re-Key after revocation

Identification and authentication procedures for re-key after revocation is same as during initial certification. This is executed only as part of a re-key operation that is approved after all investigations are performed by the PMA.

3.4 Identification and Authentication for Revocation Requests

NR-CA

In the event of the NR-CA certificate revocation due to a key compromise, the Disaster Recovery and Business Continuity plan will be executed by the NR-CA RA and the relevant teams. This operation will be authorized by the PMA director.

Subscribers

For subscribers' (Government CAs or Commercial CA) certificates revocation, the identification and authentication procedures of revocation requests involves a formal request from the respective PKI GB. Revocation request is made to the PMA by the official representatives of the PKI GB.

A revocation procedure is enforced by the PMA. It encompasses:

- the signature of a revocation request form;
- the verification of the identity of the requesters against the PKI GB nominations of the related CA.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate applications to the NR-CA are limited to the Government CAs and Commercial CA. This involves the NR-CA RA and the dully authorized representative of the respective PKI GB. The NR-CA RA is authorized to proceed with execution as long as the certificate application is part of the on-going operational cycle of the subscribing CA (Government CAs or Commercial CA), otherwise an authorization needs to be secured from the PMA.

4.1.2 Enrolment Process and Responsibilities

The NR-CA certificate operational requirements are described in internal documents including the PMA operational cycle and key ceremony documentation. Any certificate operational requirement for the NR-CA is authorized by the PMA director and executed under the supervision of the NR-CA RA function.

The certificates from the NR-CA are issued to the Government and the Commercial CAs as part of audited key ceremonies and as per an operational cycle involving the NR-CA RA function and the representatives of the respective PKI GB. The NR-CA RA executes the necessary vetting checklist for AGCE and AECE and their applicant representatives. For any certificate application to the NR-CA, the identity of the applicant representative is verified by the NR-CA RA. The NR-CA RA verifies that all data provided in the certificate application are accurate through direct interaction with the respective PKI-GB.

The PMA management cycle involves regular supervision audits performed by the PMA audit function.

The AGCE or the AECE for which a certificate has been issued by the NR-CA have an obligation to inform the NR-CA RA of any fact that materially affects the validity of a certificate. In particular, this obligation stipulates the notification of any change to its certification practices and operations, as required by the PMA governance model.

The NR-CA RA revokes Government or Commercial CAs certificates through a process involving the respective PKI GB. Identity verification is executed by the NR-CA RA for dully authorized representatives as described in chapter 3.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Certificate applications for the Government CAs or the Commercial CA are received as part of an operational cycle agreed between the PMA and the respective PKI GB. The certificate application processing involves the identity verification of the subscriber's CA applicant representative through an in-person meeting at the PMA location. Other steps are executed by the NR-CA RA including the verification of the information provided in the certificate request form against the approved CPS versions.

The NR-CA RA ensures that certificate applications are only processed if the following conditions are met:

- The existence of the applicant (AGCE or AECE) is verified using the Algerian Official Journal (Journal Officiel) which is expected to contain detailed information about the entity including its legal name and authorized official representative. The address of the government entity is also verified through an in-person visit from the NR-CA RA to relevant address;
- the subscriber CA applicant representative's identity is verified through an in-person meeting with the NR-CA RA. The NR-CA verifies the authority of the applicant representative through an attestation letter received from the respective PKI-GB;

- the certificate request is properly formatted;
- the certificate request contains the expected complete subscriber data including the official organization names;
- a formal, signed approval is received from the respective CA PKI GB;
- the CPS of the subscribing entity (AGCE or AECE) is reviewed by the NR-CA RA;
- the cycle of WebTrust internal audit successfully maintained by the PMA and the subscriber's CA.

The above verification steps are always executed by the NR-CA RA for each certification management operation with the subscribing entities.

Further details of the certificate application process are documented in the related NR-CA key ceremony documentation.

4.2.2 Approval or Rejection of Certificate Applications

Once the verification and certification evaluation processes are complete (as per the steps described in section 4.2.1) with an authorization granted by the PMA to process the certificate application, the NR-CA RA agrees with the corresponding PKI GB (AGCE or AECE) on a date for executing the certification key ceremony.

In case the certificate application is rejected, the PMA informs the corresponding PKI GB through a formal response referring to the audit report findings.

4.2.3 Time to Process Certificate Applications

No stipulation — this section intentionally left blank.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The NR-CA RA and all other required parties gather at the NR-CA primary facility to execute the NR-CA operational ceremony through which the Government CAs or the Commercial CA certificate is issued. The pre-conditions for executing the ceremony are documented in clauses 4.1 and 4.2. During the ceremony, PKI administrators in trusted roles direct commands for the NR-CA to perform a certificate signing operation.

Further details on the certificate issuing process are documented in the related NR-CA key ceremony documentation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Once the certificate is issued, the NR-CA RA ensures that the certificate issued by the NR-CA contains all data that was presented to it in the request.

Following issuance of a certificate, the NR-CA RA then handovers the issued certificate to the subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber's CA representative involved in the ceremony is responsible for checking the details of the issued certificate against the expected certificate template. The certificate is then imported to the relevant CA (Government CAs or Commercial CA) systems. The certificate is considered as formally accepted if successfully imported to the target CA systems. The certificate is then published on the target CA repository.

In case issues are raised in relation to certificate contents or to the acceptance of the certificate by the target systems, the NR-CA RA will plan and execute another ceremony in coordination with all relevant parties. These exceptions scenarios are documented in the NR-CA key ceremony documentation.

4.4.2 Publication of the Certificate by the CA

Following the acceptance of a certificate, the NR-CA operations team post the issued certificate on the Certificate Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entities or organizations are notified directly of the certificate issuance. They are indirectly notified through the update of the Repository.

4.5 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates are listed below.

4.5.1 Subscriber private key and certificate usage

Unless otherwise stated in this CP/CPS, subscribers' responsibilities are:

- Not tampering with a certificate;
- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to this CP/CPS, and with its own CP/CPS, as approved by the PMA;
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private keys;
- Not using the certificate outside its validity period, or after it has been revoked.

Refer to section 9.6.3 of this CP/CPS for complementary details.

4.5.2 Relying party public key and certificate usage

A party relying on a certificate issued by the NR-CA will:

- Use proper cryptographic tools to validate the certificate signature and validity period;
- Validate the certificate by using the CRL or the OCSP validity status information service in accordance with the certificate path validation procedure;
- Trust the certificate only if it has not been revoked and is within the validity period;
- Trust the certificate only for the signing of certificates and CRLs.

4.6 Certificate Renewal

Certificate Renewal is the act of issuing a new certificate with a new validity period while the identifying information and the public key from the old certificate are duplicated in the new certificate. Certificate renewal is not supported by the NR-CA. Only certificate re-key is supported.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

Certificate Re-key is the act of re-issuing a certificate for an existing subscriber with a new validity period, new serial number and different public key, while the remaining information from the old certificate is duplicated in the new certificate.

Certificate re-key is supported by NR-CA according to a key-change over cycle agreed with the subscribing CAs. The re-key process (including identity validation, certificate issuance and communication to relevant parties) is similar to the initial certificate application.

4.7.2 Who May Request Certification of a New Public Key

As per initial certificate issuance.

4.7.3 Processing Certificate Re-Keying Requests

As per initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per initial certificate issuance.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate modification

Certificate modifications for the Government CAs or Commercial CAs is supervised by the PMA. These changes involve discussions between the PMA and the respective PKI GB. When these changes are approved by the PMA, the respective CA CPS is amended and formally issued through the agreed channels. Considering the PMA governance model and the criticality of certificate modifications, such operation is only supported as normal certificate re-key operations.

4.8.2 Who May Request Certificate modification

Refer to section 4.8.1.

4.8.3 Processing Certificate Modification Requests

Refer to section 4.8.1.

4.8.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.8.1.

4.8.5 Conduct Constituting Acceptance of a modified Certificate

Refer to section 4.8.1.

4.8.6 Publication of the modified Certificate by the CA

Refer to section 4.8.1.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to section 4.8.1.

4.9 Certificate Revocation and Suspension

Suspension of a CA certificate is not allowed by the PMA. Only permanent certificate revocation is allowed.

4.9.1 Circumstances for Revocation

The revocation request may be triggered by the PMA or by the respective PKI GB for the AGCE or the AECE. The NR-CA RA ensures a Subordinate CA Certificate is revoked within a maximum of seven (7) days if one or more of the following events:

- The entity operating the Subordinate CA (AGCE or AECE) requests revocation in writing;
- The entity operating the Subordinate CA (AGCE or AECE) notifies the PMA that the original certificate request was not authorized and does not retroactively grant authorization;
- The PMA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

- The PMA obtains evidence that the Certificate was misused;
- The PMA is made aware that the Certificate was not issued in accordance with the provisions of this CP/CPS or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- The PMA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- CA termination plan was triggered by the PMA or an entity operating the Subordinate CA so that NR-CA or Subordinate CA ceases operations for any reason and has not made arrangements as per the CA termination plan;
- The NR-CA or Subordinate CA right to issue Certificates under the provisions of the CP/CPS expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the NR-CA CP/CPS.

Considering the criticality of the operation and its impact on the Algeria national PKI, the PMA holds an exceptional meeting inviting board members and PKI experts from the AECE and the AGCE. This meeting is organized no later than twenty-four (24) hours after the circumstances of certificate revocation were identified. The investigation outcome is presented to the PMA and PKI GB members. The outcome of this meeting is the establishment of the circumstances triggering the CA certificate revocation request and the related certificate revocation reason. The PMA may authorize the CA certificate revocation or may request additional information/evidence which shall be provided within a maximum of seventy-two (48 hours). At the end of this process, the PMA approves the CA certificate revocation and the CA certificate revocation process (in relation to the revocation circumstance) is documented as part of the PMA meeting minutes.

The certificate revocation ceremony is planned and executed not later than seventy-two (72 hours) after the CA certificate revocation is authorized by the PMA. The revocation ceremony is witnessed by members of the PMA and the PKI GBs from the AGCE and the AECE. The outcome of the ceremony will be as follows:

- The CA certificate is revoked with the right revocation reason on the NR-CA system;
- A CRL is generated by the NR-CA and placed on the target public location within 24 hours maximum from the revocation operation;
- The PMA and the respective PKI GB publish a notice within 24 hours maximum from the revocation operation containing the details of the certificate being revoked and the revocation circumstances.

After the completion of the revocation ceremony, the PKI GB responsible for the revoked CA completes the CA termination plan with proper communication towards all their affected subscribers.

4.9.2 Who Can Request Revocation

The revocation of a Certificate can be requested by:

- The Subscriber himself;
- The PMA at its own discretion (as per revocation reasons listed in section 4.9.1).

Certificate revocation requests from subscribers are only triggered through direct communication between the respective PKI GB ad the PMA.

Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify the PMA of a suspected reasonable cause to initiate the certificate revocation process.

4.9.3 Procedure for Revocation Request

The PMA provides a continuous ability for subscribers (AGCE and AECE) to submit certificate revocation requests. Considering the criticality of the operation and its impact on the Algeria national PKI, the following procedure takes place:

- The PKI GB of the entity (AGCE or AECE) calls for an exceptional meeting with the PMA advising the main subject being related to the submission of a revocation request to the PMA;
- The meeting is organized by the PMA no later than twenty-four (24) hours after receiving the request from the subscriber (AGCE or AECE).
- The subscriber discusses the circumstances of certificate revocation. The outcome of this meeting is the establishment of the circumstances triggering the CA certificate revocation request and the related certificate revocation reason. The PMA and the subscriber may request additional information/evidence from the technical teams which shall be provided within a maximum of seventy-two (72hours).
- As soon as the revocation request relevance is confirmed through a formal communication between the PMA and PKI GB, the subscriber submits a formal revocation request to the NR-CA RA. This is approved by the PMA.
- The certificate revocation ceremony is planned and executed not later than seventy-two (72 hours) after the CA certificate revocation is authorized by the PMA. The revocation ceremony is witnessed by members of the PMA and the respective PKI GB of the subscriber. The outcome of the ceremony will be as follows:
  - The subscriber CA certificate is revoked with the right revocation reason on the NR-CA system;
  - s generated by the NR-CA and placed on the target public location within 24 hours maximum from the revocation;
  - The PMA and the respective PKI GB publish a notice within 24 hours maximum from the revocation operation containing the details of the certificate being revoked and the revocation circumstances.

Certificate problems reporting:

Subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports via ANCE.Certification.Problem@agce.dz.

The NR-CA discloses instructions related to certificate revocation and certificate problem reporting on its public repository. For any certificate problem report, the reporter is requested to include his contact details, suspected abuse and related domain name. The NR-CA RA begins the investigation of a certificate problem report within 24 hours of receipt and decide whether revocation or other appropriate actions are required.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Revocation requests are processed by the PMA timely after a decision for revocation is made and in all circumstances within the timeframes listed under section 4.9.1 of this CP/CPS.

4.9.5 Time within which CA must process the revocation request

For certificate problem reports, the PMA begins investigations within 24 hours from receipt. The PMA initiates communication with the affected subscriber and where appropriate, with Algerian law enforcement authorities. A preliminary communication on the certificate problem is sent to the third party that filled the certificate problem report and to the subscriber. Refer to section 4.9.1 for further details on the investigations and processing of the certificate problem executed by the PMA.

4.9.6 Revocation Checking Requirement for Relying Parties

Revocation information is offered to relying parties through CRLs published on a publicly available web server or through its OCSP responder. Relying parties shall use any of these methods while processing a certificate issued by the NR-CA.

4.9.7 CRL Issuance Frequency

The NR-CA update and reissue CRLs (i) once every six months and (ii) within 24 hours after revoking a Subordinate CA Certificate. The value of the nextUpdate field of CRL issued by the NR-CA is set to 184 days beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 Online Revocation/Status Checking Availability

The NR-CA offers an OCSP responder that conforms to RFC 6960 and whose certificate is signed by the NR-CA. The OCSP certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by the NR-CA.

4.9.10 Online Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

The NR-CA OCSP responder supports the HTTP GET method.

The NR-CA updates information provided via its OCSP responder (i) every six months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

The NR-CA OCSP responder that receive a request for status of a certificate that has not been issued (″unused ″), do not respond with a "good" status for such Certificates. OCSP responders for CAs which are not Technically Constrained, in line with Section 7.1.5, do not respond with a "good" status for such Certificates.

The NR-CA operations team monitors the OCSP responder for requests for "unused" serial numbers as part of its security monitoring procedures and any such case will trigger further investigation.

4.9.11 Other Forms of Revocation Advertisements Available

The NR-CA only uses OCSP and CRL as methods for publishing certificate revocation information.

4.9.12 Special Requirements related to Key Compromise

If the PMA discovers, or has a reason to believe, that there has been a compromise of the NR-CA private key, this will be considered as a disaster scenario and the NR-CA business continuity plan is invoked.

Refer to section 4.9.1 for circumstances of subscribing CA certificate revocation.

4.9.13 Circumstances for Suspension

Certificate suspension is not supported by the NR-CA.

4.9.14 Who Can Request Suspension

No applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CRLs are published by the NR-CA on a public repository which is available to relying parties through HTTP protocol queries.

The NR-CA OCSP responder exposes an HTTP interface accessible to relying parties.

Revocation entries on a CRL or OCSP responses are not removed until after the expiry date of the revoked certificates.

4.10.2 Service Availability

The repository including the latest CRL are available 24 hours a day and 7 days a week, with an availability percentage of minimum 99 % over one year.

The NR-CA operations team operates and maintains the CRL and OCSP capabilities with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The PMA maintains a 24X7 ability to respond internally to high-priority certificate problem report as described in section 4.9.3 of this CP/CPS.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Not applicable. Subscribing CAs are part of the Algerian PKI governance system and are de-facto subscribers of the NR-CA.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are not escrowed. The NR-CA does not support key escrow services.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable. The NR-CA does not provide session key encapsulation and recovery services.

5 Facility, Management, Operational and Physical Controls

This clause describes non-technical security controls used by the NR-CA operations team to perform the functions of key generation, certificate issuance, certificate revocation, audit, and archival.

The NR-CA security management program complies with the CA/Browser Forum's Network and Certificate System Security Requirements. This program includes:

1. Physical security and environmental controls;
2. System integrity controls, including configuration and change management, patch management, vulnerability management and malware/virus detection/prevention;
3. Maintaining an inventory of all assets (PKI and non-PKI) and manage the assets according to their classification;
4. Network security and firewall management, including port restrictions and IP address filtering;
5. User management, separate trusted-role assignments, education, awareness, and training; and
6. Logical access controls, activity logging and monitoring, and regular user access review to provide individual accountability.
7.

The PMA conducts an annual Risk Assessment on the NR-CA that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements in place to counter such threats.

Based on the Risk Assessment, the NR-CA operations team develops, implements, and maintains its security management plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.

5.1 Physical Controls

The PMA ensures that appropriate physical controls are implemented on the NR-CA (hosting) premises for their activities. These physical controls are documented in internal PMA documentations: “Logical/physical access control policies” and “Physical site requirements”. These controls are enforced by the PMA as part of regular internal audits performed by the PMA compliance function on the NR-CA operations.

The NR-CA‘s premises physical controls include the following:

5.1.1 Site Location and Construction

All critical components of the PKI solution are housed within a highly secure facility operated by the AGCE. The whole facility foundations and basement ceiling are built with concrete and reinforced with steel rebar. Physical security controls are enforced so that access of unauthorized persons is prevented through five layers of physical security. When this layered access control is combined with the physical security protection mechanisms such as guards, intrusion sensors and CCTV, it provides robust protection against unauthorized access to the NR-CA systems.

5.1.2 Physical Access

The NR-CA systems are protected by multi-tiered physical security measures, with access to the lower tiers only possible by first gaining access through the higher tiers. The inner controlled areas are accessible only via several gated security checkpoints. Technical physical security controls are continuously enforced including two-factor authentication to move from one layer to another, protection sensors, CCTV and video recordings. Procedural controls are also enforced including the continuous escort of pre-authorized visitors to the site. All these controls protect the facility from unauthorized access and are monitored on a 24x7x365 basis.

5.1.3 Power and Air Conditioning

The design of the facility hosting the NR-CA provides UPS and backup generators with enough capability to support the NR-CA operations in power failure circumstances. UPS units and stand-by generators are available for the entire facility. A fully redundant air-conditioning system is installed in the areas hosting the NR-CA systems. All these systems ensure that the NR-CA equipment continuously operate within the manufacturers’ range of operating temperatures and humidity.

5.1.4 Water Exposures

The PMA has taken reasonable precautions to protect the NR-CA facility and NR-CA systems and minimize the impact of water exposure. These include installing the NR-CA equipment on elevated floors with moisture detectors.

5.1.5 Fire Prevention and Protection

The PMA follows leading practices and applicable safety regulations in Algeria to ensure the NR-CA facility is monitored 24x7x365 and equipped with fire and heat detection equipment. Fire suppression equipment is installed within dedicated areas and automatically activates in the case of fire, and can be manually activated, if necessary. Additional fire prevention and protection enforced in the NR-CA facility include:

- Fire-resistant walls and pillars;
- Fire and smoke detectors deployed in the facility and which are monitored by the facility alarm systems;
- A sufficient number of fire extinguishers deployed in the facility.

5.1.6 Media Storage

Electronic, optical and other storage media are subject to the multi-layered physical security and are protected from accidental damage (water, fire, electromagnetic interference). Audit and backup storage media are stored in a secure fire-proof safe and duplicated and stored in the NR-CA disaster recovery location.

5.1.7 Waste Disposal

All waste paper and storage media created within the secure facility are destroyed before discarding. Paper media is shredded using a cross-hatch shredder. The following procedure applies for removable computer media:

- Authorization is granted for the destruction of any removable computer media;
- The media is erased then physically destroyed if no longer required;
- Record of this media destruction are maintained;
- Media can then be released for disposal.

5.1.8 Offsite Backup

Full and incremental backups of the NR-CA systems are taken regularly to provide enough recovery information when the recovery of the NR-CA system is necessary. At least one full backup and several incremental backups are taken daily in accordance with documented backup policies and procedures enforced by the NR-CA operations team. Adequate back-up facilities ensure that backup copies are transferred to the disaster recovery location where they are stored with the same physical, technical and procedurals controls that apply to the primary facility.

The backup and recovery system is tested at least once a year in accordance with the NR-CA Disaster Recovery Plan.

5.2 Procedural Controls

The PMA ensures that the appropriate procedural controls are implemented for NR-CA activities to provide reasonable assurance of the trustworthiness and competence of the staff, and of the satisfactory performance of their duties in the field of PKI governance and operations. The procedural controls include the following:

5.2.1 Trusted Roles

All members or staff with functional roles in the key management operations, including but not limited to, administrators, security officers, and system auditors, or any other role that materially affects such operations, are considered as serving in a trusted position; i.e. trusted operatives.

The PMA is responsible for due diligence in vetting of all candidates to serve in trusted roles, to determine their trustworthiness and competence, prior to the candidate’s employment in their respective role.

At minimum, the following trusted roles are established with the appropriate segregation of duties:

- PKI system administration: Trusted roles authorized to install and configure the NR-CA and to perform back-up, recover and maintenance operations. Also authorized to configure other users in the target

NR-CA systems;

- PKI system operation: Trusted roles authorized to execute the NR-CA operational cycle and is involved in operations such as subscribers' certification operations and NR-CA CRLs generation;
- Key management operation: Trusted roles cleared to operate as key custodians and hold key material and secrets necessary for the execution of NR-CA operational ceremonies;
- HSM administrator: Trusted roles authorized to hold HSM activation data and secrets necessary for the HSM operation;
- Security operation: Trusted roles authorized to collect and view the audit logs generated by the NR-CA systems as part of the continuous monitoring of the NR-CA systems;
- Audit operation: Trusted roles authorized to review the NR-CA systems audit logs as part of regular internal compliance audits.

5.2.2 Number of Persons Required Per Task

The PMA ensures segregation of duties for critical NR-CA functions to prevent operators from holding too many privileges, thereby becoming potential malicious agents. User access and role management is enforced to limit operational staff to only conducting the operations they have been authorized and cleared for. Dedicated user access forms are continuously maintained by the NR-CA operations manager. These forms are used as part of the regular internal audits performed by the PMA audit and compliance function on the NR-CA operations.

Key splitting techniques are defined and enforced as part of the NR-CA key management policies and procedures. This ensures that no single individual may gain access to NR-CA private keys. At a minimum two key custodians together with HSM administrators are involved in NR-CA key operations such as NR-CA system start-up and NR-CA system shutdown, key backup or key recovery operation.

The PMA ensures that all operational activity performed by NR-CA staff in trusted roles is logged and maintained in a verifiable and secure audit trail.

5.2.3 Identification and Authentication for Each Role

Before exercising the responsibilities of a trusted role:

- The PMA confirms the identity and history of the employee by carrying out background and security checks;
- When instructed through the internal PMA processes, the facility operator (AGCE) issues an access card to each staff who needs to physically access equipment located in the secure enclave;
- NR-CA dedicated staff (system administrators) issue the necessary IT system credentials for NR-CA staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

ANCE ensures separation of duties among the following work groups:

- Operating personnel (manages operations on certificates, key custodians, helpdesk etc.)
- Administrative personnel (system admins, network admins, HSM admins etc.)
- Security personnel (enforce security measures)
- Audit personnel (review audit logs)

5.3 Personnel Controls

The PMA mandates the implementation of security controls for the duties and roles of the staff members in charge of NR-CA activities.

The NR-CA personnel security controls include the following:

5.3.1 Qualifications, Experience and Clearance requirements

All NR-CA personnel fulfilling trusted roles are selected based on skills, experience, integrity and background check. The following checks are performed:

- Obtaining testimonials from references;
- CV contents verification;
- Specific security clearances as required;
- Validation of degrees, certifications, or credentials/awards submitted by the candidate;
- Misrepresentations or omission of relevant data.

The requirements related to minimum qualifications are documented in the PMA governance document and other internal PMA documents. While performing any critical operation on the NR-CA systems, trusted roles are held by Algerian national citizen.

5.3.2 Background Check Procedures

All employees filling trusted roles are selected based on integrity, background investigation and security clearance. The PMA ensures that these checks are performed once yearly for all personnel holding trusted roles.

5.3.3 Training Requirements

The PMA makes available relevant technical personnel to perform their respective role. A comprehensive training curriculum is prepared and delivered as part of the establishment of the NR-CA operations. This training is regularly updated and delivered on a yearly basis to NR-CA personnel.

The training curriculum is delivered by a mix of NR-CA experienced staff and third parties specialized in security and PKI. It is designed to address the needs of the various trusted roles involved in operating and delivering the NR-CA services. In particular, the training curriculum covers basic and advanced topics necessary for the NR-CA RA and PKI administrators (i.e. validation specialists) to master the RA processes and related verification and vetting processes.

The topics covered in the training are:

- PKI theory and principles
- PKI environmental controls and security policies
- PKI RA processes including vetting and verification procedures
- PKI operational processes
- PKI products hands-on training
- PKI trusted roles management
- PKI disaster recovery and business continuity procedures
- PKI latest trends and technology developments

The PMA maintains documentation on all personnel who attended training and monitors the satisfaction levels of the trainers on all trainees. Examination tests are organized at the end of the training sessions and certificates delivered to the staff that pass successfully the examination tests. No trusted role, including the validation specialists, will be allowed to operate without passing successfully the examinations tests.

5.3.4 Retraining frequency and requirements

The training curriculum is delivered to all NR-CA personnel. The training content is reviewed and amended on a yearly basis to reflect the latest leading practices and NR-CA configuration changes.

5.3.5 Job rotation frequency and sequence

The PMA ensures that any change in the NR-CA staff will not affect the operational effectiveness, continuity and integrity of the NR-CA services.

5.3.6 Sanctions for unauthorized actions

For the purpose of maintaining accountability on NR-CA personnel, the PMA sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems, according to the relevant human resources policy and procedures, and the applicable Algerian law.

5.3.7 Independent contractor requirements

The PMA does not employ independent contractors as part of its operations and trusted roles are exclusively held by Algerian nationals.

Whenever independent contractors and third parties are involved for maintenance and operational support purposes, the PMA ensures that the engaged personnel are subject to the same background check, security control and training as permanent CA staff.

5.3.8 Documentation supplied to personnel

The PMA documents all training material and make it available to NR-CA personnel. The PMA also ensures that key documentation related to NR-CA operations is made available to the personnel. This includes, at a minimum, this CP/CPS document, security policies and the technical documentation relevant to every trusted role.

5.4 Audit Logging Procedures

The NR-CA systems maintains an audit for material events and operations executed on the NR-CA systems. This includes key life cycle management, including key generation, backup, storage, recovery, destruction and the management of cryptographic devices, the CA and OCSP responder. Security audit log files for all events relating to the security of the CA, RA and OCSP responder are generated and preserved. These logs are reviewed by the NR-CA security monitoring team and are also reviewed as part of the regular internal audits performed by the PMA on NR-CA operations.

The PMA ensures that the following controls are implemented:

5.4.1 Types of Event Recorded

Audit log files are generated for all events relating to the security and services of the NR-CA CA. Where possible, the audit logs are automatically generated and where not possible, a logbook or paper forms are used. The audit logs, both electronic and non-electronic, are retained by the NR-CA operations team and may be made available during compliance audits.

Following events occurring in relation to the NR-CA operations are recorded:

1. NR-CA key life cycle management events, including:
   a. Key generation, backup, storage, recovery, archival and destruction
   b. Cryptographic device life-cycle management events
2. NR-CA and NR-CA Subscribing CAs Certificate life-cycle management events, including:
   a. Certificate requests, re-key requests, and revocation
   b. All issued certificates including revoked and expired Certificates
   c. Verification activities evidence (e.g. date, time, calls, persons communicated with)
   d. Acceptance and rejection of certificate requests
   e. Issuance of certificates
   f. CRL updates (including OCSP entries updates where applicable)
3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts
   b. PKI and security system actions performed
   c. Security profiles and configuration changes
   d. User management operations
   e. System platform issues (e.g. crashes), hardware failures
   f. Firewall and router activities
   g. Entries and exists from the CA facility

Log entries will include at minimum the following elements:

1. Date and time of entry
2. Identity of the person/system making the log entry
3. Description of the entry

5.4.2 Frequency for Processing and Archiving Audit Logs

The PMA ensures that designated personnel review log files at regular intervals in order to validate log integrity and ensure timely identification of anomalous events. At a minimum, the following audit log review cycle is implemented by the PMA:

- NR-CA application and security audit logs are reviewed by the security operations team on daily basis as part of the regular daily operations;
- On a monthly basis, senior PKI operations management reviews the applications and systems logs to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly;
- On a quarterly basis, senior PKI operation management reviews the physical access logs and the user management on the NR-CA systems with an objective to continuously validate the on-going physical and logical access policies;
- At minimum once a year , the PMA audit and compliance function executes an internal audit of the NR-CA operations. Samples of the audit logs produced since the last audit cycle are requested by the PMA as part of this internal audit.
- Evidence of audit log reviews, outcome of the review process and executed remediation actions are collected and archived.

5.4.3 Retention Period for Audit Log

The NR-CA operations team ensures that the audit logs are maintained and retained for a period not less than 2 years as following:

- NR-CA certificate and key lifecycle management event records (as set forth in Section5.4.1(1)) after the later occurrence of:
  1. The destruction of the NR-CA Private Key; or
  2. The revocation or expiration of the NR-CA certificate

- NR-CA Subscribing CAs Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the revocation or expiration of any Subscriber CA Certificate;
- Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

These audit logs may be made available to auditors upon request.

5.4.4 Protection of Audit Log

Audit logs are protected by a combination of physical, procedural and technical security controls as follows:

- The NR-CA systems generates cryptographically protected audit logs;
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived;
- The access control policies enforced on the NR-CA systems ensures that read access only is granted to personnel having access to audit logs as part of their operational duties;
- Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective NR-CA operations personnel.

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the NR-CA audit log:

- Backup media are stored locally in the NR-CA's main site in a secure location;

- A second copy of the audit log data and files are stored in the disaster recovery site that provides similar physical and environmental security as the main site.

5.4.6 Audit Collection System (internal vs. external)

The audit log collection system is an integral system of the NR-CA internal support systems. Refer to section 5.4.4 for the protection of audit logs.

5.4.7 Notification to Event-causing Subject

Where an event is logged by the NR-CA systems, no notice is required to be given to the individual, or application that caused the event.

5.4.8 Vulnerability Assessments

The NR-CA systems and infrastructure are subject to regular security assessment as follows:

- Quarterly automated vulnerability scan of all public and internal IP addresses of NR-CA core and supporting PKI systems. This regular self-assessment activity is executed by security personnel part of the NR-CA operations team;
- On an annual basis and before the yearly WebTrust audit is planned, the PMA ensures a third-party independent vulnerability assessment and penetration testing is conducted on the NR-CA systems.

The outcome of the regular assessments and identified issues are made available to the higher NR-CA PKI operation management who is responsible to organize and oversee the execution of the remediation by the respective teams.

Evidence of the vulnerability assessment and penetration testing activities execution are collected and archived by the relevant NR-CA personnel.

The PMA operational cycle also includes an annual risk assessment which targets the identification of potential new internal and external threats, assess the likelihood and potential damage of these threats and assess the adequacy of the existing implemented controls. Based on the risk assessment results (which coincides with the annual external vulnerability and penetration testing exercise), the NR-CA higher PKI operational management will develop and present a security plan to the PMA seeking the necessary approvals to proceed with the remediation implementation.

5.5 Records Archival

5.5.1 Types of records archived

The NR-CA operations team ensures that at least the following records are archived:

- All documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof ;
- Key ceremony documentation and related verification information;

5.5.2 Retention period for archive

The PMA retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for 7 years after any certificate issued by the NR-CA based on that documentation ceases to be valid.

5.5.3 Protection of archive

Records are archived in such a way that they cannot be deleted or destroyed. Controls are in place to ensure that only authorized personnel can manage the archive without diminishing integrity, authenticity, or confidentiality of the records.

Archived records are protected by a combination of physical, procedural and technical security controls as follows. Archived records are securely maintained using the access control mechanisms enforced by the NR-CA support systems. These policies ensure that the appropriate access rights are granted to personnel having access to all archived records as part of their operational duties.

5.5.4 Archive backup procedures

Only one version of each digital archive is maintained in the primary and disaster recovery facilities of the NR-CA. The NR-CA operations team use backup, restore and archive procedures that document how the archive information is created, transmitted and stored.

5.5.5 Requirements for Time-stamping of records

All recorded and archived events include the date and time of the event taking place. The time of NR-CA systems is synchronized with the time source of a GPS clock. Further, the NR-CA operations team enforce a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection system (internal or external)

Only authorized and authenticated staff are allowed to access archived material. The NR-CA operations team use the NR-CA backup, restore and archive procedures that document how the archive information is created, transmitted and stored. These procedures also provide information on the archive collection system.

5.5.7 Procedures to obtain and verify archive information

Refer to clause 5.5.6.

5.6 Key Changeover

To minimize impact of key compromise, the NR-CA key is changed with a frequency that ensures each CA part of the Algeria PKI hierarchy (from NR-CA to issuing CAs) has validity period greater than the maximum lifetime of Subscriber certificate after the latest Subscriber certificate issuance.

Refer to clause 6.3.2 of this CP/CPS document for key changeover frequency.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

The PMA has a Disaster Recovery and Business Continuity Plan that documents the procedures necessary to restore the NR-CA services in case of business failure, disaster or security compromise. The PMA may disclose the plan to its auditors upon request.

The PMA annually tests, reviews, and enhances the Disaster Recovery and Business Continuity Plan. The following topics are covered in the plan:

- The conditions for activating the plan
- Emergency procedures
- Fallback procedures
- Resumption procedures
- A maintenance schedule for the plan
- Awareness and education requirements
- The responsibilities of the individuals
- Recovery time objective (RTO)
- Regular testing of contingency plans
- The CA’s plan to maintain or restore the CA’s business operations in a timely manner following interruption to or failure of critical business processes
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location
- What constitutes an acceptable system outage and recovery time
- How frequently backup copies of essential business information and software are taken
- The distance of recovery facilities to the CA’s main site and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.2 Computing resources, software, and/or data are corrupted

The NR-CA PKI operations team implements the necessary measures to ensure full recovery of the NR-CA services in case of a disaster, corrupted servers, software or data. Communication with the PMA occurs to authorize the triggering of the required incident recovery procedures.

The NR-CA disaster recovery and business continuity document lists the incidents that affects the NR-CA operations and that require the execution of specific recovery procedures. If the NR-CA operational capabilities are affected due to corrupted servers, software or data, the recovery procedures will involve the disaster recovery site.

The NR-CA disaster recovery and business continuity plan is tested at least once a year including failover scenarios to the disaster recovery location.

5.7.3 Entity private key compromise procedures

Compromise of the NR-CA private key(s), or of the associated activation data is considered as a mission-critical incident that triggers a process and related procedures detailed in the NR-CA business continuity and disaster recovery plan.

Considering the criticality of such compromise situation and its impact on the Algeria national PKI, the PMA holds an exceptional meeting inviting board members and PKI experts from AECE and AGCE. Refer to sections 4.9.1 and 4.9.3 for further details.

5.7.4 Business continuity capabilities after a disaster

In case of a disaster, corrupted servers, software or data, the NR-CA disaster recovery and business continuity plan is triggered in order to restore the minimum NR-CA required operational capabilities, in a timely fashion. In particular, the plan targets the recovery of the following services either on the primary site or the disaster recovery site:

- Public repository where CRLs and NR-CA certificates are published;
- NR-CA OCSP service.

Failover scenarios to the NR-CA disaster recovery location are made possible considering the NR-CA backup system that enables the continuous replication of critical NR-CA data from the primary site to the disaster recovery site.

The NR-CA disaster recovery and business recovery plan is tested at least once a year including failover scenarios to the disaster recovery site. The plan demonstrates the recovery of the NR-CA critical services at the disaster recovery location within a maximum of twelve (12) hours RTO.

The business continuity and disaster recovery plan includes at a minimum the following information:

1. Conditions for activating the plan;
2. Fall-back and resumption procedures;
3. The responsibilities of the individuals involved in the plan execution;
4. Recovery time objective (RTO);
5. Recovery procedures;
6. The plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes;
7. Key termination plan (in case of NR-CA key compromise);
8. Procedures for securing the main facility to the extent possible during the period following a disaster and up to recovery of operations in a secure environment in either the main, or secondary site.

5.8 CA or RA Termination

Considering the nature of the NR-CA service, its termination is not an applicable event. Refer to clauses 4.9 and 5.7 of this CP/CPS for NR-CA key compromise and revocation.

6 Technical Security Controls

This clause defines the security measures the PMA takes to protect its cryptographic keys and activation data (e.g. PINs, passwords, and key access tokens).

6.1 Key Pair Generation and Installation

The NR-CA implements and documents key generation procedures in accordance with this CP/CPS.

6.1.1 Key Pair Generation

NR-CA

The NR-CA key generation ceremony is planned in advance and full dry runs are executed before the live ceremonies can be planned. The ceremony is subject to the formal authorization of the PMA director. The ceremony requires HSMs that meet the requirements of FIPS 140-2 Level 3 and dedicated machine to be setup by authorized NR-CA personnel only. The detailed key ceremony activities are documented in the NR-CA key ceremony procedure and related ceremony log. The ceremony involves the execution of technical procedures through which the NR-CA personnel setup the NR-CA software and trigger the NR-CA key pair generation and self-signed certificate creation through the NR-CA HSM. The trusted personnel involved in the NR-CA key generation ceremony selects their own secrets and HSM activation data is then generated. All NR-CA private key material, secrets and activation data is maintained in tamper evident envelopes during the entire lifecycle of the NR-CA private key.

The NR-CA Key Generation Ceremony is witnessed by a WebTrust qualified auditor. The activities performed in each NR-CA key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a period of time defined in the NR-CA backup and archive procedures. After a successful ceremony execution, the auditor issues an unqualified audit report.

Subscribing CAs

The PMA oversees the establishment of the Government CAs and Commercial CAs (subscribing CAs) and approves their respective ceremonies through the PMA governance model and operational cycle. The key generation ceremonies for the subscribing CAs are also witnessed by a WebTrust qualified auditor. The security measures that are in place for key generation of the subscribing CAs are documented in their respective CP/CPS.

The NR-CA software rejects the processing of certificate request from a Subscribing CA if the requested public key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

6.1.2 Private key delivery to subscriber

The NR-CA does not generate private keys for Subscribers.

6.1.3 Public key delivery to certificate issuer

For the Government CAs or Commercial CAs (Subscribing CAs), the public key certificate is available as part of the certificate application processing. Refer to clauses 4.3 and 4.4 of this CP/CPS document for further details.

6.1.4 CA public key delivery to relying parties

The NR-CA public key is provided within the NR-CA self-signed certificate and is published on the NR-CA public repository.

6.1.5 Key sizes

NR-CA

The minimum size for the NR-CA Root CA Keys using the RSA SHA-256 algorithm is 4096 bits.

Subscribing CAs

The minimum size for Subscribing CAs Keys using the RSA SHA-256 algorithm is 4096 bits.

6.1.6 Public key parameter generation and quality checking

NR-CA

NR-CA's public Key module generation is done with HSM devices that conforms to FIPS 186-2 for random generation and primality checks. The NR-CA operations team references the Baseline Requirements Section 6.1.6 on quality checking.

Subscribing CAs

Same provisions shall apply for subscribing CAs public key parameter generation.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

NR-CAs

Private Keys corresponding to the NR-CA Certificates are not used to sign Certificates except in the following cases:

- Self-signed Certificates to represent the NR-CA itself;
- Certificates for Subordinate CAs;
- And certificates for NR-CA OCSP responder.

Subscribing CAs

Private Keys corresponding to the Subscribing CAs Certificates shall not be used to sign Certificates except in the following cases:

- Certificates for Issuing CAs;
- And certificates for Subscribing CAs OCSP responder.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The NR-CA operations team implements physical and logical safeguards to prevent unauthorized certificate issuance. The NR-CA private key never exists during normal operations outside cryptographic hardware that are certified/validated for FIPS 140-2 Level 3. Backup copies are taken for business continuity purposes and are also held securely inside FIPS 140-2 Level 3 cryptographic hardware. The protection of the NR-CA private key must consist at all times of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA private key. When encryption is used (i.e. to create backups of the CA private key), algorithms and key-lengths are used that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

NR-CA

The NR-CA relies on secure cryptographic device in the form of Hardware Security Modules (HSM) certified/validated for FIPS 140-2 Level 3. The NR-CA HSMs are maintained and held securely within the most inner and secure zone of the NR-CA facility.

Subscribing CAs

NR-CA provisions shall apply to subscribing CAs that shall use certified/validated for FIPS 140-2 Level 3.

6.2.2 Private key (n out of m) multi-person control

NR-CA

The NR-CA private keys are continuously controlled by multiple authorised persons, trusted roles in relation to NR-CA private keys (and related secrets) management are documented in the NR-CA key ceremony document and other internal PMA documentation.

NR-CA personnel are assigned to the trusted roles by the PMA ensuring segregation of duties and enforcing the principles of multi control and split knowledge. Multi-person control of the NR-CA private key is achieved using an “m-of-n” split key knowledge scheme. A certain number of persons ‘m’ (at least two (2)), out of ‘n’ persons (three (3) persons), the total number of key custodians, need to be concurrently present, together with HSMs administrators and a PMA staff, to activate or re-activate the NR-CA private key. The PMA keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it will keep track of the renewed tokens and/or password distribution.

Subscribing CAs

Same provisions, related to NR-CA private key protection and multi-person control, shall apply to subscribing CAs.

6.2.3 Private key escrow

Private keys of the NR-CA are not escrowed.

Private keys of the subscribing CA shall not be escrowed. Private key backup NR-CA

The NR-CA private key is backed up and held stored safely in exclusive safes maintained in the most inner security zones of the PKI facilities. Backup operations are executed as part of the NR-CA key generation ceremonies. The NR-CA key is backed up under the same dual control and split knowledge as the primary key. The recovery operation of the backup key is subject to the same dual control and split knowledge principles.

The NR-CA private keys are physically transported from the primary facility to the DR facility using a dedicated HSM handling and key handling procedure part of the overall NR-CA key ceremony documentation. Dedicated personnel in trusted roles participate in the transport operation which is escorted by security guards. Refer to clause 6.2.2 for further details.

Subscribing CAs

The backup and management of subscribing CAs private keys shall be subject to the same security measures and controls that apply to the NR-CA private key backup.

6.2.4 Private key archival

The NR-CA operations team does not archive the NR-CA private keys.

6.2.5 Private key transfer into or from a cryptographic module

NR-CA

The NR-CA uses FIPS 140-2 Level 3 certified/validated HSMs for the primary and disaster recovery facilities. NR-CA private key and related secret material are backed up as part of the audited key generation ceremonies. Key backup operations are executed through HSM token-to-token operations ensuring encrypted key backups are generated the enforcement of dual control and split knowledge mechanisms. The recovery operations are subject to the same dual control and split knowledge principles. Key backups are transported to the backup PKI facility where recovery operations may be executed as part of the Disaster Recovery and Business Continuity plan. The transfer and recovery operations are subject to the same dual control and split knowledge principles.

If during a transfer operation, the NR-CA private key has been compromised and potentially communicated to an unauthorized person or organization, then the PMA will trigger the key compromise procedure as part of the Disaster Recovery and Business Continuity plan. All certificates issued by the transferred private key will be revoked.

Subscribing CAs

Same provisions, related to NR-CA private key transfer to/from cryptographic modules, shall apply to subscribing CAs private key transfer.

6.2.6 Private key storage on cryptographic module

No further stipulation other than those stated in clauses 6.2.1, 6.2.2, 6.2.4 and 6.2.6.

6.2.7 Method of activating private key

NR-CA

The NR-CA private key is activated inside the HSM as part of audited key ceremonies attended by several trusted personnel and relevant PMA personnel. The principles of dual control and split knowledge are enforced so that each trusted personnel involved in the ceremony holds his own set of secrets/activation data/key share. The NR-CA key remain active only for the duration of the activity requiring the NR-CA activation (e.g. certification, CRL generation). The details of NR-CA private keys activation are documented in the NR-CA key ceremony documentation.

Subscribing CAs

Subscribing CAs activate their own private keys. Same security measures and methods to activate NR-CA private keys shall apply to activating the private keys of subscribing CAs.

6.2.8 Method of deactivating private key

NR-CA

The HSMs used for the NR-CA key ceremony are deactivated at the end of the ceremony which prevents any further use of the private keys. This activity applies to the principles of dual control and split knowledge and is always be witnessed by the relevant personnel (PMA, auditor). The HSMs are safely powered off at the end of the ceremony and all material used during the ceremony is put back in their respective safes.

Subscribing CAs

Same provisions, related to NR-CA private key deactivation, shall apply to subscribing CAs private key deactivation.

6.2.9 Method of destroying private key

NR-CA

At the end of their lifetime, the NR-CA private keys are irrevocably destroyed in the presence of at least three (3) trusted NR-CA personnel and at least one (1) PMA representative.

The NR-CA keys are destroyed after permanent removal from any hardware module the keys are stored on.The hardware module will be then reset or returned to its factory state.

The NR-CA private key destruction outside the context of the end of its lifetime applies to investigation and special authorization from the PMA.

The key destruction process is detailed in the dedicated key ceremony documentation. Any associated records are archived, including a report evidencing the key destruction process.

Subscribing CAs

Same provisions, related to NR-CA private key destruction, shall apply to subscribing CAs private key destruction.

6.2.10 Cryptographic Module Rating

NR-CA

The NR-CA cryptographic modules are certified/validated to FIPS 140-2 Level 3.

Subscribing CAs

The NR-CA cryptographic modules are certified/validated to FIPS 140-2 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

See clause 5.5 for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods

The NR-CA certificate has a validity period at least greater than the last Subscriber certificate it issued, augmented with a grace period that takes into account the NR-CA key ceremony procedure.

The NR-CA self-signed certificates is valid for twenty-five (25) years, with a key usage period for signing subscriber certificates of eight (8) years.

The subscribing CA’s certificates are valid for seventeen (17) years, with a key usage period for signing subscriber certificates of eight (8) years.

6.4 Activation Data

6.4.1 Activation data generation and installation

NR-CA

The NR-CA private key and HSM activation data is generated during the NR-CA private key generation ceremony. Refer to clauses 6.1.1 and 6.2.8 of this CP/CPS for further details.

Subscribing CAs

The subscribing CA’s activation data generation and installation shall be subject to the same security controls as the NR-CA activation data generation and installation.

6.4.2 Activation data protection

NR-CA

The NR-CA key management policy and ceremony procedures ensure that the principles of dual control and split knowledge are permanently enforced to protect NR-CA keys and HSMs activation data. During NR-CA key ceremonies, activation data are permanently under the custody of the designated NR-CA trusted personnel. Refer to clause 6.1 and 6.2 for further details.

Subscribing CAs

The subscribing CA's activation data protection shall be subject to the same security controls as the NR-CA activation data protection.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

NR-CA

The NR-CA operations is subject to security controls documented in the NR-CA policy manual. The NR-CA is operated according to the following minimum security arrangements:

- Separation of duties and dual controls for CA operations;
- Physical and logical access control enforcement;
- Audit of application and security related events;
- Continuous monitoring of NR-CA systems and end-point protection;
- Backup and recovery mechanisms for NR-CA operations;
- Hardening of NR-CA servers' operating system according to leading practices and vendor recommendations;
- In depth network security architecture including perimeter and internal firewalls, web application firewalls and including intrusion detection systems;
- Proactive patch management as part of the NR-CA operational processes.
- The NR-CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

The PMA organizes regular (at minimum once a year) internal audit to monitor the NR-CA operations against the target security controls.

Subscribing CAs

Subscribing CA shall be operated according to the same security controls as listed above for the NR-CA.

6.5.2 Computer Security Rating

The NR-CA computer running the certification authority software is positively tested in accordance with the requirements of NATO Publications of SDIP-27 Level B (TEMPEST).

6.6 Life Cycle Technical Controls

NR-CA

6.6.1 System Development Controls

Purchased hardware or software are to be shipped in a sealed, tamper-proof container, and installed by qualified personnel. Hardware and software updates are to be procured in the same manner as the original equipment. Dedicated NR-CA trusted personnel are involved to implement the required NR-CA configuration according to documented operational procedures.

Applications are tested, developed and implemented in accordance with industry leading development and change management practices. No software (or patches) or hardware is deployed on live systems before going through the change and configuration management processes enforced by the NR-CA operations team.

All NR-CA hardware and software platforms are hardened considering leading practices and vendor recommendations.

6.6.2 Security Management Controls

The hardware and software used to set up the NR-CA is dedicated to performing only CA-related tasks. There are no other applications, hardware devices, network connections or component software, which are not part of the PKI, connected to or installed on CA hardware.

The NR-CA equipment is scanned for malicious code on first use and periodically thereafter. Authorised personnel must ensure up-to-date virus definition databases in place before each NR-CA usage.

Refer to clause 6.6.1 for further details.

6.6.3 Life Cycle Security Controls

Refer to 6.5.1.

6.7 Network security controls

NR-CA

The NR-CA is operated as an offline CA not connected to any network. The NR-CA equipment and secret material are maintained in security safe located in the innermost security zone of the NR-CA facility.

The NR-CA repository and OCSP responder are online systems supporting the NR-CA operations and enabling service provision to relying parties in compliance with the provisions of this CP/CPS. A Defence in depth network security architecture is enforced including perimeter and internal firewalls, web application firewalls, end point protection, including intrusion detection systems. The network is segmented into several zones based on a defined conceptual and functional architecture for the NR-CA systems. These controls and technologies limit the services allowed to and from the NR-CA online services.

The PMA ensures regular vulnerability testing is conducted on the NR-CA online services. The PMA also ensures that at least once a year, penetration testing is conducted on the NR-CA connected systems, by an independent third-party.

Subscribing CAs

The subscribing CA’s network protection shall be subject to the same network security controls as the NR-CA network.

6.8 Time-stamping

NR-CA

It is the machine time that is used for generating the archived record.

There is no NTP service available for the NR-CA offline machine. The time is the NR-CA's machine time that is verified by the quorum in charge of activating the NR-CA during the ceremonies.

An NTP server is available as part of the NR-CA connected infrastructure. It is used to synchronize the time of the connected servers that are part of the NR-CA connected infrastructure including the OCSP service and online repository.

Subscribing CAs

Same provisions as the once applied for the NR-CA.

7 Certificates, CRL, and OCSP Profiles

7.1 Certificate Profile

NR-CA self-signed certificate profile

Root CA Certificate Profile					
Field	CE[1]	O/M[2]	CO[3]	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA Signature.	CA signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption

Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[300]** Months	Suggested validity for the Root CA is 25 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code
					elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Subject Properties					

SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the Root CA public key
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
BasicConstraints	True	M			This extension MUST be marked CRITICAL
CA		M	S	True	TRUE for CA Certificates

[1] CE = Critical Extension. O/M: O = Optional, M = Mandatory. CO = Content: S = Static, D = Dynamic

Government CA certificate profile

Government CA Certificate Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA’s Signature.	Root CA’s Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	

NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Government CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL

Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties					
KeyUsage	False	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
id-kp-clientAuth		M	S	True	
Policy Properties					
CertificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.1.1.1	National ROOT CA CP/CPS OID
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.ance.dz/repository/cps	
BasicConstraints	True	M			
CA		M	S	True	TRUE for CA Certificates
pathLenConstraint		O	S	1	

Government TLS CA Certificate Profile

Government TLS CA Certificate					
Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA’s Signature.	Root CA’s Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				

CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Government TLS CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key	

					Key length: 4096 (RSA)	
Extensions			M			
Authority Properties						
AuthorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
	AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain <download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
Extended Key Usage		False	M			
	id-kp-serverAuth		M	S	True	
	id-kp-clientAuth		O	S	True	
Policy Properties						
Certificate Policies		False	M			
	PolicyIdentifier		M	S	2.16.12.3.1.1.1	National Root CA CP/CPS OID

policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.ance.dz/repository/cps	
Certificate Policies	False	M			
PolicyIdentifier		M	S	2.23.140.1.2.2	BR SSL OV reserved OID
BasicConstraints	True	M	S		
CA		M	S	True	TRUE for CA Certificates
pathLenConstraint		O	S	1	

Government CS CA

Government CS CA Certificate Profile					
Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA’s Signature.	Root CA’s Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)

OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Government CS CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	False				
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field

	AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
	AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key usage Properties						
KeyUsage		True	M	S		
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
Extended Key Usage		False	M			
	id-kp-codeSigning		M	S	True	
Policy Properties						
Certificate Policies		False	M			
	PolicyIdentifier		M	S	2.16.12.3.1.1.1	National ROOT CA CP/CPS
	policyQualifiers:policyQualifierId		O	S	id-qt 2	
	policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.ance.dz/repository/cps	
Certificate Policies		False	M			
	PolicyIdentifier		M	S	2.23.140.1.4.1	BR CS Reserved OID
BasicConstraints		True	M			
	CA		M	S	True	TRUE for CA Certificates
	PathLenConstraint		O	S	1	

Government SMIME CA

Government SMIME CA Certificate Profile					
Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA's Signature.	Root CA's Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	

NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Government SMIME CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	False				
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL

Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
Extended Key Usage	False	M			
id-kp-emailProtection		M	S	True	
Policy Properties					
Certificate Policies	False	M			
PolicyIdentifier		M	S	2.16.12.3.1.1.1	National Root CA CP/CPS
policyQualifiers:policyQualifier Id		O	S	id-qt 1	
policyQualifiers:qualifier:cPSur i		O	S	https://ca.pki.ance.dz/repository/cps	
BasicConstraints	True	M	S		
CA		M	S	True	TRUE for CA Certificates
PathLenConstraint		O	S	1	

Government TS CA certificate profile

Governement TS CA Certificate Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA’s Signature.	Root CA’s Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				

CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Government TS CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key	

					Key length: 4096 (RSA)	
Extensions			M			
Authority Properties						
AuthorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
	AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
ExtendedKeyUsage		False				
	id-kp-timeStamping		M	S	True	
Policy Properties						
Certificate Policies		False	M			
	PolicyIdentifier		M	S	2.16.12.3.1.1.1	National Root CA CP/CPS
	policyQualifiers:policyQualifierId		O	S	id-qt 1	

policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.ance.dz/repository/cps	
Certificate Policies	False	M			
PolicyIdentifier		M	S	2.23.140.1.4.2	BR CS Reserved OID (TSA)
BasicConstraints	True	M			
CA		M	S	True	TRUE for CA Certificates
pathLenConstraint		O	S	1	

Commercial CA certificate profile

Commercial CA Certificate Profile					
Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA’s Signature.	Root CA’s signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-

					alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Commercial CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except

					for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the subjectPublicKey
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
id-kp-clientAuth		M	S	True	
Policy Properties					
CertificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.1.1.1	National Root CA CP/CPS OID

policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.ance.dz/repository/cps	
BasicConstraints	True	M			
CA		M	S	True	TRUE for CA Certificates
pathLenConstraint		O	S	1	

Commercial TS CA certificate profile

Commercial TS CA Certificate Profile					
Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA’s Signature.	Root CA’s signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			

CountryName		M	S	DZ	Encoded according to “ISO 3166-1-
					alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[204]** Months	Suggested validity for the Subordinate CA is 17 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Commercial TS CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Authority Properties					

AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.ance.dz	OCSP responder URL
AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		O	S	http://ca.pki.ance.dz/repository/cert/root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ca.pki.ance.dz/repository/crl/root_ca.crl	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the subjectPublicKey
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage properties	False	M			
id-kp-timeStamping		M	S	True	
Policy properties					
CertificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.1.1.1	National Root CA CP/CPS

	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	S	https://pki.ance.dz/repository/cps	
Certificate Policies		False	M			
	PolicyIdentifier		M	S	2.23.140.1.4.2	BR CS Reserved OID (TSA)
BasicConstraints		True	M			
	CA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		O	**S**	**1**	

7.1.1 Version number(s)

X.509 v3 is supported and used for all certificates related to the NR-CA (see tables in clause 7.1).

7.1.2 Certificate extensions

X.509 v3 extensions are supported and used as indicated in the certificates profiles as described in Algeria PKI – Certificate Templates (see tables in clause 7.1).

7.1.3 Algorithm object identifiers

Algorithms OID conform to IETF RFC 3279 and RFC 5280 (see table in clause 7.1).

7.1.4 Name forms

Name forms are in the X.500 distinguished name form as implemented in RFC 3739.

The Subject Attributes used are provided in the certificates profiles (see tables in clause 7.1).

7.1.5 Name constraints

Name constraints are not supported.

7.1.6 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739 & RFC 5280.

OIDs used are provided in the certificate profiles as described in the tables in clause 7.1.

All subscriber's CA certificates issued by the NR-CA containing a policy identifier indicating compliance with CA/Browser Forum Baseline Requirements referenced in section 1.6.3, are issued and managed in accordance with those Requirements.

7.1.7 Usage of Policy Constraints extension

Policy Constraints extension is not supported.

7.1.8 Policy qualifiers syntax and semantics

The use of policy qualifiers defined in RFC 5280 is supported.

Used policy qualifiers are provided in the certificate profiles as described in the tables in clause 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension

Certificate policies extensions must be processed as per RFC 5280.

7.2 CRL Profile

In conformance with the IETF PKIX RFC 5280, the NR-CA supports CRLs compliant with:

- Version numbers supported for CRLs;
- CRL and CRL entry extensions populated and their criticality.

CRL Profile					
Field	CE[4]	O/M[5]	CO[6]	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's signature value
TbSCertList	False				
Version	False	M			
Version		M	S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	
CommonName		M	S	National Root CA	

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	thisUpdate		M	D	<creation time>	
	NextUpdate		M	D	<Creation time> + **[184]** days	
RevokedCertificates		False	O			
Certificate						
	CertificateSerialNumber		M	D	Serial of the revoked certificates	
	revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
	crlEntryExtension	False	M			
	CRLReason		M	D	As per RFC 5280	Identifies the reason for the certificate revocation
	Invalidity Date		O	D	Date when the certificate is supposed to be invalid	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
CRLExtensions		False	M			
	AuthorityKeyIdentifier	False	M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey of the CA public key
	CRL Number	False	M	D		Sequential CRL Number

[4] CE = Critical Extension.
O/M: O = Optional, M = Mandatory. CO
= Content: S = Static, D = Dynami

7.2.1 Version number(s)

The NR-CA supports X.509 version 2 CRLs (see 7.2 above)

7.2.2 CRL and CRL entry extensions

The profile of the CRL is provided 7.2 above.

7.3 OCSP Profile

The OCSP profile complies with the requirements of RFC 6960.

The OCSP response signing certificate profile is as follows:

OCSP Response Signing Certificate Profile					
Field	CE[7]	O/M[8]	CO[9]	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	National Root CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[12]** Months	Suggested validity for the OCSP certificate is one year
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE NATIONALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
stateOrProvinceName		M	S	Algiers	UTF8 encoded.
CommonName		M	S	National Root CA OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			

	KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey
Authority Properties						
AuthorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
Key Usage Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
	nonRepudiation		M	S	True	
extKeyUsage		False	M			
	id-kp-OCSPSigning		M	S	True	
Policy Properties						
id-pkix-ocsp-nocheck		False	M	S		
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.16.12.3.1.1.1	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.ance.dz/repository/cps	

[7] CE = Critical Extension.
O/M: O = Optional, M = Mandatory. CO = Content: S = Static, D = Dynamic

7.3.1 Version number(s)

The NR-CA OCSP responder conform to RFC 6960.

7.3.2 OCSP extensions

No stipulation.

8 nce Audit and Other Assessments

8.1 Frequency or circumstances of assessment

The PMA ensures that the NR-CA operations are subject to internal and external audits.

The internal audits are planned and executed at minimum once a year by the PMA audit function. This internal audit is part of the PMA operational cycle and the PMA ensures that mitigations are implemented timely for the audit findings.

External audits are planned and executed by an independent WebTrust practitioner according to the WebTrust audit scheme. As requested by the CA/B forum, before issuing Publicly-Trusted Certificates, the NR-CA will have successfully completed a point-in-time readiness assessment. The point-in-time readiness assessment has been completed prior to CA operations (including the Root Key Generation Ceremony). A period-of-time audit has been then conducted within ninety (90) days of the CA operations start.

The period during which the CA issues Certificates is divided into a contiguous sequence of audit periods. An audit period do not exceed one (1) year in duration.

8.2 Identity / qualifications of assessor

The external audits will be performed by qualified auditors that fulfil the following requirements:

- Independence from the subject of the audit
- Ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's relationship to assessed entity

For internal audit, the PMA audit function is independent of the NR-CA operations team.

External auditors are independent third party WebTrust practitioners.

8.4 Topics covered by assessment

The NR-CA is audited for compliance to the following standard:

- WebTrust for Certification Authorities Principles And Criteria
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- Webtrust Principles And Criteria For Certification Authorities – Code Signing Baseline Requirement

Refer to section 8.1 for the periodicity of the audits. Refer to section 8.2 for the assessor's qualifications.

8.5 Actions taken as a result of deficiency

Issues and findings resulting from the assessment are reported to the PMA.

The final audit report includes the issues and findings as well as the agreed corrective action plan and target date for resolution.

The issues and findings are tracked until resolution by the PMA. Additional audits are planned and carried out sufficient to reach full compliance.

8.6 Communication of results

The internal audit reports are communicated to the PMA and are not disclosed to non-authorised third parties.

External audit reports are published on the NR-CA public repository.

8.7 Self-audits

The PMA, through its compliance function, monitors and strictly controls its adherence to the procedures listed in this CP/CPS document and to the Baseline Requirements by performing self-audits on at least yearly basis. Refer to sections 8.1 and 8.6 for further details.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Applicable fees, if any, are to be agreed upon by the PMA and the subscribers.

9.1.2 Certificate Access Fees

No fee may be charged for access to issued certificates.

9.1.3 Revocation or Status Information Access Fees

No fee will be charged for Certificate revocation or status information access.

9.1.4 Fees for Other Services

ANCE may charge for other services depending on business needs and subject to the PMA approval.

9.1.5 Refund Policy

No refunds for any charged fees.

9.2 Financial Responsibility

9.2.1 Insurance coverage

The PMA ensures that the NR-CA is covered by existing government insurance provisions.

It is the sole discretion and responsibility of relying parties to ensure an adequate level of insurance coverage to cover risks of using NR-CA certificate or services.

9.2.2 Other assets

The PMA maintains sufficient financial resources to support the continuous operations of the NR-CA and ensure the fulfilment of the NR-CA duties as per the provisions of this CP/CPS.

This provision applies also to the subscribing CAs through their respective PKI GB.

9.2.3 Insurance or warranty coverage for end-entities

No warranty coverage is available for end entities. Refer to section 9.6.1 for warranties.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The ANCE guarantees the confidentiality of any classified data being the following:

- Subscriber’s personal information that are not part of certificates or CRLs issued by NR-CA;
- Correspondence between the subscriber and the NR-CA RA during the certificate management processing (including the collected subscriber’s data);
- Contractual agreements between the ANCE and its suppliers;
- ANCE internal documentation (business processes, operational processes, ….);
- Employee confidential information.

9.3.2 Information not within the scope of confidential information

Any information not defined as confidential (refer to section 9.3.1) is deemed public. This includes the information published on the NR-CA repository.

9.3.3 Responsibility to protect confidential information

The ANCE protects confidential information through adequate training and policy enforcement with its employees, contractors and suppliers.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

The ANCE observes personal data privacy rules and privacy rules as specified in the present CP/CPS. The ANCE implements these provisions through the NR-CA RA.

Refer to section 9.4.2 for the scope of private information and to section 9.4.3 for the items that are not considered as private information.

Both private and non-private information can be subject to data privacy rules if the information contains personal data.

Only limited trusted personnel are permitted to access subscribed private information for the purpose of certificate lifecycle management.

The ANCE respects all applicable privacy, private information, and where applicable trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention and disclosure of non-public information.

Private information will not be disclosed by the ANCE to subscribers (Government CAs and Commercial CA) except for information about themselves and only covered by the contractual agreement between the ANCE and the subscribers.

The ANCE will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the ANCE releases private information, ANCE will ensure through reasonable means that this information is not used for any purpose apart from the requested purposes. Parties granted access will secure the private data from compromise, and refrain from using it or disclosing it to other third-parties. Also, these parties are bound to observe personal data privacy rules in accordance with the relevant laws in the people's democratic republic of Algeria.

All communication channels with the ANCE preserve the privacy and confidentiality of any exchanged private information. Data encryption is used when electronic communication channels are used with the NR-CA systems. This includes:

- The communications between the NR-CA RA systems and the subscribers;
- Sessions to deliver certificates.

9.4.2 Information treated as Private

All personal information that is not publicly available in the content of a certificate or CRL are considered as private information.

9.4.3 Information not Deemed Private

Information included in the certificate or CRL is not considered as private.

9.4.4 Responsibility to protect private information

The ANCE employees, suppliers and contractors handle personal information in strict confidence under the ANCE contractual obligations that at least as protective as the terms specified in section 9.4.1.

9.4.5 Notice and consent to use private information

The ANCE ensures that collected personal information is used for the purpose of certificate life cycle management only as consented by the subscribers.

Unless otherwise stated in this CP/CPS, the ANCE Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

9.4.6 Disclosure Pursuant Judicial or Administrative Process

The ANCE will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. Refer to section 9.4.1 for more details.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The PMA owns and reserves all intellectual property rights associated with the NR-CA’s databases, repository, the NR-CAs digital certificates and any other publication originating from the PMA including this CP/CPS.

The NR-CA uses software from third party PKI products suppliers. This software remains the intellectual property of the product suppliers and its usage by the NR-CA bound by licenses agreements between the PMA and these suppliers.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The ANCE warrants that their NR-CA procedures are implemented in accordance with this CP/CPS, and that any certificates issued under this document are in accordance with the stipulations specified.

By issuing a Certificate, the NR-CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement;
- All Application Software Suppliers with whom the Root CA will enter into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier;
- and all Relying Parties who reasonably rely on a Valid Certificate.

The NR-CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the NR-CA has complied with the Baseline Requirements and its CP/CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

- **Right to Use Domain Name or IP Address:** Right to Use Domain Name or IP Address: Not applicable for the NR-CA as per the provisions of this CP/CPS;
- **Authorization for Certificate:** That, at the time of issuance, the NR-CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the NR-CA’s CP/CPS;
- **Accuracy of Information:** That, at the time of issuance, the NR-CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the NR-CA’s CP/CPS;
- **No Misleading Information:** That, at the time of issuance, the NR-CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate’s subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the NR-CA’s CP/CPS;
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the NR-CA’s CP/CPS;
- **Subscriber Agreement:** That, if the NR-CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- **Status:** That the NR-CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;
- **Revocation:** That the NR-CA will revoke the Certificate for any of the reasons specified in these Requirements

The NR-CA is responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA’s compliance with these requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these requirements, as if the NR-CA were the Subordinate CA issuing the Certificates

9.6.2 RA Representations and Warranties

The PMA warrants that it performs RA functions as per the stipulations specified in this CP/CPS.

9.6.3 Subscriber Representations and Warranties

The ANCE warrants that each subscriber signs a subscriber's agreement that lists the subscriber's obligations. The Subscriber agreement enforces the below minimum obligations:

- Secure private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key;
- Use Subscriber Certificate only for its intended uses as specified by this CP/CPS;
- Notify the ANCE in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been lost, accessed by another individual, or compromised in any other manner;
- Use the Subscriber Certificate that does not violate applicable laws in the people's democratic republic of Algeria; and
- Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use of the Subscriber Certificate according to the subscriber's termination plan.

The ANCE requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the NR-CA and the Certificate Beneficiaries. Prior to the issuance of a Certificate, the ANCE SHALL obtain, for its express benefit and the Certificate Beneficiaries, either:

- The Applicant's agreement to the Subscriber Agreement with the ANCE, or
- The Applicant's acknowledgement of the Terms of Use.

The ANCE implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request. The Subscriber Agreement or Terms of Use contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the PMA, both in the certificate request and as otherwise requested by PMA in connection with the issuance of the Certificate(s) to be supplied by the NR-CA;
- **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- **Use of Certificate**: To use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;
- **Reporting and Revocation**: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

- **Responsiveness**: An obligation to respond to PMA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the PMA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the NR-CA CP/CPS, or the Baseline Requirements.

9.6.4 Relying parties Representations and Warranties

Relying Parties who rely upon the certificates issued under the NR-CA shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Verify the Validity by ensuring that the Certificate has not Expired;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- Ensure that the Certificate has not been revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determine that such Certificate provides adequate assurances for its intended use.

9.6.5 Representations and Warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

Within the scope of the law of the people's democratic republic of Algeria, and except in the case of fraud, or deliberate abuse, the ANCE cannot be held liable for:

- The accuracy of any information contained in certificates except as it is warranted by the subscriber that is the party responsible for the ultimate correctness and accuracy of all data transmitted to the NR-CA with the intention to be included in a CA certificate;
- indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures;
- wilful misconduct of any third-party participant breaking any applicable laws in the people's democratic republic of Algeria, including, but not limited to those related to intellectual property protection, malicious software, and unlawful access to computer systems;
- for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of the NR-CA services;
- any form of misrepresentation of information by TSPs or relying parties on information contained in this CP/CPS or any other documentation made public by the PMA and related to the NR-CA services.

9.8 Limitations of Liability

Limitations on Liability:

- The PMA will not incur any liability to Subscribers to the extent that such liability results from their negligence, fraud or wilful misconduct;

- The PMA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this CP/CPS for any use other than in accordance with this document. Subscribers will immediately indemnify the ANCE from and against any such liability and costs and claims arising there from;
- The PMA will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Subscribers are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by the PMA;
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscriber's breach of Subscriber's agreement;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- The PMA denies any financial or any other kind of responsibility for damages or impairments resulting from the NR-CA operation.

9.9 Indemnities

This CP/CPS does not include any claims of indemnity.

9.10 Term and termination

9.10.1 Term

The present CP/CPS is approved by the PMA and remains in force until amendments are published on the NR-CA repository and relevant communication towards the subscribers.

9.10.2 Termination

Amendments to this document are applied and approved by the PMA and marked by an indicated new version of the document. Upon publishing on the NR-CA repository, the newer version becomes effective. The older versions of this document are archived by the NR-CA on its repository.

9.10.3 Effect of Termination and Survival

The PMA coordinates communications towards the subscribers in relation to the termination (and related effects) of this document.

9.11 Individual notices and communications with participants

Notices related to the present CP/CPS may be addressed by the subscribers to the PMA. Such communications and exchanges may be in writing or electronic. If in writing, the communications and exchanges shall happen using organizations letterhead and signed by the official representatives. Electronic communication may be in emails using the agreed email addresses.

For all other communications, no further stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA reserves the right to change this CP/CPS as and when needed. The PMA will incorporate any such change into a new version of this document and, upon approval, publish the new version. The new document will carry a new version number.

9.12.2 Notification Mechanism and Period

Upon publishing on the NR-CA repository, the newer version of the CP/CPS becomes effective. The older versions of this document are archived on the NR-CA repository. The PMA coordinates communication towards the subscribers in relation to the amendments of this CP/CPS and related effects.

9.12.3 Circumstances Under Which OID Must Be Changed

Major changes to this CP/CPS that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the OID or qualifier (URL). The PMA coordinates proper communication to the subscribers.

9.13 Dispute Resolution Provisions

All disputes associated with the provisions of this CP/CPS and the NR-CA services, shall be first addressed by the PMA legal function. If mediation by the PMA legal function is not successful, then the dispute will be adjudicated by the relevant courts of Algeria.

9.14 Governing Law

The Algerian government laws governs the enforceability, construction, interpretation, and validity of this CP/CPS.

9.15 Compliance with applicable law

This CP/CPS and the provisions of NR-CA certification services are compliant to relevant and applicable laws of the Republic of Algeria. In particular:

- Law 15-04 fixing “*les règles générales relatives à la signature et à la certification électroniques*”.
- Décret exécutif N°16-134

9.16 Miscellaneous provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate the NR-CA CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of the ANCE.

9.16.3 Severability

If any provision of this CP/CPS is determined to be invalid or unenforceable, the other sections remains in effect until this CP/CPS is updated.

In the event of a conflict between the Baseline Requirements and any regulation in Algeria, the PMA may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Algeria. This applies only to operations or certificate issuances that are subject to that Law. In such event, the PMA will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by the PMA. The PMA will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS. Any modification to the PMA practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The ANCE is not liable for any failure or delay in their performance under the provisions of this CP/CPS due to causes that are beyond their reasonable control., including, but not limited to unavailability of interruption or delay in telecommunications services.

9.17 Other Provisions

Not applicable.