ECONOMIC AUTHORITY OF ELECTRONIC CERTIFICATION

AECE PKI

Commercial Certification Authority – CP/CPS

Version 1.3

FEBRUARY 2021

Document management

Information

Group of document	Governance model
Title	Commercial Certification Authority – CP/CPS
Project reference:	Algeria National PKI
Annex:	n.a.

Version control

Version	Date	Description / Status	Responsible
V0.1	18/03/2019	Document preparation	AECE
V0.2	17/04/2019	Proofreading & formatting	AECE
V0.3	29/04/2019	Complete draft for customer	AECE
V0.4	30/09/2019	Typos, feedback from customer.	AECE
V0.5	25/10/2019	Additional feedback from customer.	AECE
V0.6	08/12/2019	Version addressing latest comments and for final review comments from AECE	AECE
V0.7	20/02/2020	Addressing auditor comments and changed Commercial CA DN as per final decision from PKI management	AECE
V1.0	26/03/2020	Included final URLs and corrected few typos	AECE
V1.1	20/01/2021	Added final AECE address and contact information + several enhancements to accommodate feedback from previous reviews with WebTrust auditor	AECE
V 1.2	31/01/2021	Legal and financial revision part	AECE
V 1.3	24/02/2021	Addressing ANCE (PMA) feedback	AECE

Document Signoff

Version	Date	Responsible	Validated by	Reviewed and Approved by
V 1.3	25/02/2021	AECE	AECE PKI GB 24/02/2021	ANCE (PMA) 25/02/2021

Table of contents

1 Introduction

The present Certificate Policy and Certification Practice Statement (hereinafter, CP/CPS) of the **Economic Certification Authority of Algeria** (hereinafter, COM-CA) applies to the certification services of the COM-CA.

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 COM-CA. Such clauses are denoted as “clause 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 COM-CA with regard to all services available during the lifetime of certificates issued by the COM-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 COM-CA can be obtained from the PKI Governance Board (PKI GB), 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. As the National PKI governance body, the ANCE’s mandate is to operate the Policy Management Authority (PMA).

The Government Authority for Electronic Certification (Authorité Gouvernementale de Certification Electronique – AGCE) is established by the Algerian Government to operate the GOV-CA 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 CA: Intermediate CA certified by the Root CA.

  The Government CA certifies two issuing CAs as follows:

  - Corporate CA: Technically controlled CA that will issue certificates to natural persons (government employees) and legal persons (government entities).

- Infrastructure (Devices) CA: Technically controlled CA that will issue certificates to non-natural entities, such as servers and VPN device certificates.

Additional CAs may be added in the Government domain. These CAs will be operated by government TSPs and will be certified by the Government CA. As part of its mandate delegated from the PMA, the AGCE oversees and audits the establishment of these government TSPs.

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 this and other CP and CPS documents relating to certificates within AGCE PKI. It interacts closely with the PMA to implement the Government 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 under the Economic PKI branch. In this context, the ARPCE operates as the Authority for Economic Certification (Autorité Economique de Certification Electronique – AECE). The AECE implements and operates the COM-CA as an intermediate CA certified by the NR-CA. 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.

There are two options for TSPs to establish certification services under the COM-CA:

- Option 1: 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 (issued by the COM-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.

- Option 2: This is the scenario of a TSP that have a bigger scope and requires flexibility to operate a more scalable hierarchy. In this scenario, the provisions of this CP/CPS allow the TSP to establish a two-level PKI hierarchy under the COM-CA, first level being an unconstrained subordinate CA certified by the COM-CA and second level being one or more technically constrained issuing CAs certified by the TSP unconstrained subordinate CA.

In both options, the AECE is responsible for the supervision and authorization of the TSP that shall successfully complete an authorisation process. The details of the supervision and authorization process from the AECE is documented in the “AECE supervision system for TSPs under the commercial domain” document.

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.

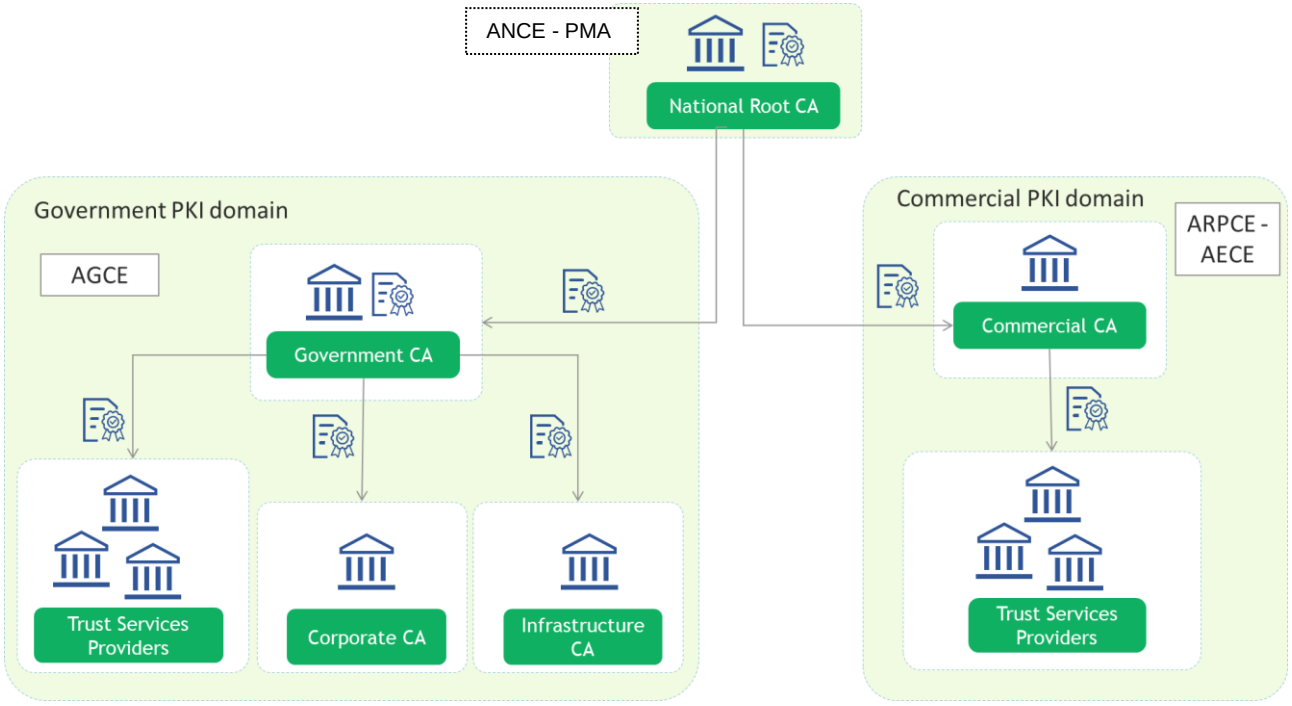

Figure 1: The Algerian National PKI hierarchy

The issuance of a certificate by the Government or Commercial CA respectively, will endorse a TSP to become part of the Algeria National PKI governance model.

The present CP/CPS relates to the COM-CA certification services. The COM-CA only issues CA certificates to TSP that are under the control of Commercial entities.

1.2 Document Name and Identification

This document is titled “AECE – Commercial Intermediate CA CP/CPS” and is referenced in related documents as [AECE COM-CA CP/CPS].

The COM-CA will also use the OID 2.16.12.3.3.1.1 to identify this document.

1.3 PKI Participants

Several parties make up the participants of this COM-CA PKI. The parties mentioned hereunder including the NR-CA, the COM-CA, subscribers and relying parties are collectively called PKI participants.

1.3.1 Certification Authorities

The COM-CA is a Certification Authority operated by AECE from dedicated facilities located in Algeria. The COM-CA issues certificates in accordance with this CP/CPS and ensures the availability of all services pertaining to the issued certificates, including the issuing, revocation and status verification services.

The AECE operates with a governance and operating model relying on two complementary structures:

- PKI Governance Board: Operating as the governance function for the AECE PKI. It groups the necessary functions for this purpose including the policy, compliance and design functions. The PKI Management Board (hereinafter, PKI GB) provides strategic direction and continuously supervises the PKI operations team. The AECE PKI GB operating cycle includes interactions with

the PMA which is responsible for overseeing the operations of the COM-CA through regular supervision audits conducted by the PMA audit and compliance function.

- PKI operations: This technical operations structure is responsible for operating the COM-CA and its online services. It falls under the management and supervision of the PKI GB.

The COM-CA is certified by the Algeria National Root CA (NR-CA), under the supervision of the PMA. The PMA is responsible for the Algeria national PKI framework which includes the Root CPS which the AECE CP/CPS (this document) shall comply to. 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 and other trust services offered by TSPs certified under the COM-CA.

1.3.2 Registration Authorities

The AECE operates the RA function of the COM-CA. The RA function falls within the PKI operations structure and responsible for processing certificate management requests of the CAs (TSPs) under the COM-CA. When a TSP requests for the creation of a CA certificate under the COM-CA, it is the RA function responsibility to validate the request before communicating with the PKI GB in order to seek a formal approval of at least 2 members to proceed with the creation of the CA certificate. See section 3 and 4 for further details.

1.3.3 Subscribers

Subscribers are commercial TSPs operating CAs under the COM-CA. A subscriber has the final responsibility of the lifecycle management of the certificates it issues. The provisions of this CP/CPS allow two (2) types of CA hierarchies for the subscriber to setup certification services under the COM-CA. In the first type, the COM-CA will certify a technically constrained issuing CA operated by the subscriber. In the second type, the subscriber can setup a two-level PKI hierarchy under the COM-CA, first level being an unconstrained subordinate CA certified by the COM-CA, and second level being one or more technically constrained issuing CAs certified by the TSP unconstrained subordinate CA. In this case, the subscriber shall undergo independent WebTrust audit in addition to complying with the relevant supervisory requirements from AECE.

A subscriber shall meet its contractual obligations with the AECE that covers the policy and practices requirements stated in this CP/CPS. Further details on the contractual obligations between subscribers and the AECE are documented in the “AECE supervision system for TSPs under the commercial domain” document.

The subscribers:

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

The CAs operated by the subscribers are referred hereafter as the “subscribing CAs or Subordinate CAs”.

1.3.4 Relying Parties

Relying parties are entities including natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

The relying parties shall always verify the validity of a digital certificate issued by the COM-CA using the COM-CA Certificate Validity Status Service (e.g. CRL, webpage, OCSP), prior to relying on information featured in said certificate.

The COM-CA certificate is published on the COM-CA repository (see clause 2).

1.3.5 Other participants

There are no other participants for this CA.

1.4 Certificate Usage

Certain limitations apply to the usage of certificates issued by the COM-CA that includes the ones stated hereunder.

1.4.1 Appropriate certificate uses

The certificates issued by the COM-CA can be used to

- Issue certificates for issuing CAs
- Issue certificates for end-entities, in accordance with the certificate types accepted in the Algeria PKI domain
- Issue certificate revocation lists (CRLs), containing the list of subscribers' revoked certificates.
- Issue OCSP certificates for the COM-CA OCSP service

1.4.2 Prohibited certificate uses

Certain limitations apply to the usage of certificates issued by the COM-CA as stated in this CP/CSP:

- Subscribing CAs are not authorized to use their certificates to issue certificates or to support services that are out of the scope of what is described in their CP/CPS as approved by the AECE.
- It is prohibited to use the COM-CA certificate to sign end-user or server certificates (other than OCSP server).

1.5 Policy Administration

1.5.1 Organization Administering the Document

The AECE PKI GB bears responsibility for the drafting, publishing, maintenance, and interpretation of this CP/CPS. This CP/CPS shall be approved by the PMA, since any policy approved by the PMA has to ultimately comply with the provisions of the NR-CA CP/CPS.

The AECE PKI GB is comprised of members with relevant PKI policy experience and appointed to conduct the following PKI policy administration tasks:

- Drafting, amending, maintaining and interpreting this CP/CPS
- Approve the publishing of this CP/CPS and its updates after the completion of a review process with the PMA to continuously ensure this CP/CPS complies with the NR-CA CP/CPS
- Publishing this CP/CPS and its revisions

- Conducting regular reviews on the COM-CA operations

1.5.2 Contact details

The AECE PKI GB can be contacted at the following address:

Autorité Economique de Certification Electronique

Cyber Park Sidi Abdellah, BT D,

Rahmania, Zeralda, Alger

Tel: +213 (0) 21 47 02 05

+213 (0) 21 47 77 77

Fax: +213 (0) 21 47 01 97

Email: Info@aece.dz

The AECE PKI GB 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 COM-CA by sending an email to: reports@aece.dz

The COM-CA 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 AECE PKI GB bears responsibility for the drafting, publishing, maintenance, and interpretation of this CP/CPS. This CP/CPS shall be approved by the PMA as well, since it has to ultimately comply with the provisions of the National Root CA CP.

1.5.4 CPS approval procedures

A dedicated process involves the AECE PKI GB reviewing the initial version of this CP/CPS and any subsequent updates. Amendments shall either be in the form of a document containing an amended form of the CP/CPS or an update notice. The PKI GB as well as the PMA formally approves the newer version of the document.

1.6 Definitions and Acronyms

1.6.1 Definitions

The following is a list of term definitions and acronyms used in the present 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.

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 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

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 COM-CA 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 CPS, the COM-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 AECE operates the RA for the COM-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 —The specifications requirement document which set the terms and conditions for providing of electronic certification services

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 PSCEs)
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 defers 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 Trust Service Principles and Criteria for Certification Authorities
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
- CA/B Forum Network and Certificate System Security Requirements
- Algerian Law 15-04 on "*signature électronique et certification*", fixant les règles générales relatives à la signature et à la certification électroniques
- Decree 135 (décret exécutif N°16-135 fr);
- Decree 134 (décret exécutif N°16-134 fr).

2 Publication and Repository Responsibilities

2.1 Repositories

The AECE maintains an online repository of documents where it makes certain disclosures about the COM-CA practices, procedures and the content of some of its policies. Published information include:

- This CP/CPS
- TSP CP
- PKI disclosure statement
- Audit reports
- Certificates issued by the COM-CA
- NR-CA certificate
- Subscriber Agreement for Subordinate CA

The repository is publicly accessible at https://pki.aece.dz/repository

The AECE reserves its right to make available any additional information as it sees fit.

2.2 Publication of Certification Information

As part of the online repository, the COM-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 AECE will at all times make available the current versions of the COM-CA CP/CPS document on its public repository.

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

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

The COM-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.

With regard to the COM-CA activities, and due to their sensitivity, the COM-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 COM-CA publishes digital certificate status information in intervals indicated in this CP/CPS. The provision of COM-CA issued electronic certificate validity status information is a 24x7x365 service.

- The COM-CA publishes CRLs including any changes since the publication of the previous CRL, at regular intervals.
- The COM-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 COM-CA.

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

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

The COM-CA operations team ensures that the CP/CPS of COM-CA is reviewed at least once annually and makes appropriate changes so that the COM-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 PKI GB approval.

2.4 Access controls to repositories

Public read-only access is given to the COM-CA repository. Security controls are implemented on the repository by the COM-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 Type of names

The COM-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 **Commercial CA** DN is as follows:

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

The **Commercial CA OCSP** certificates bear the following DN:

- CountryName : DZ
- stateOrProvinceName : Algiers
- OrganizationName : AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE
- CommonName : Commercial CA OCSP

Commercial TSP CAs have a DN structured as follows:

- CountryName : DZ
- OrganizationUnitName (optional): Name of the TSP organization unit
- OrganizationName : Name of the TSP organisation
- LocalityName (optional): TSP locality
- CommonName : Meaningful name of the TSP 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

AECE 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 COM-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

AECE 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 COM-CA is validated against the exact meaningful denomination, as agreed with the official representatives of the TSP.

The certificates are requested from the COM-CA RA by duly delegated representatives of the TSP. A registration procedure is enforced by the COM-CA RA to duly perform identity verifications of the authorized representatives. This process encompasses:

- Signature of a registration / certificate request form by the TSP representative
- COM-CA RA using the official channels (e.g. chamber of commerce, Algerian Official Journal) to validate relevant information related to the TSP, including the official representative
- Any additional paperwork to be provided by the TSP representative and deemed necessary by the COM-CA RA, as part of the verification process
- review and validation by the PKI GB of the requesting entity CPS;
- site visit by a COM-CA RA representative to the requesting entity site in order to validate the address;
- In-person verification of the identity of the requesters nominated by the TSP representative.

3.2.3 Non-verified Subscriber Information

All subscriber information contained within certificate issued by the COM-CA shall be verified by AECE RA.

3.2.4 Authentication of Individual Identity

The COM-CA does not issue certificates for individuals.

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 in the Algeria National PKI 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-Keying

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 PKI GB.

3.4 Identification and Authentication for Revocation Requests

The identification and authentication procedures of revocation requests involves a formal request from duly authorized representative of the TSP. A revocation procedure is enforced by the AECE COM-CA RA. It encompasses:

- The signature of a revocation request form by the authorized representative
- The verification of the identity of the requesters against the information available to the COM-CA RA (provided during the TSP enrolment)
- Communication with the TSP to provide reasonable assurances that the TSP official representative authorized the revocation operation. Such communication, depending on the circumstances, may include one or more of the following: telephone, e-mail or courier service

4 Certificate Life-Cycle Operational Requirements

The COM-CA issues certificates to TSPs that are within the Commercial domain.

The TSP for which a certificate has been issued by the COM-CA has an obligation to inform the COM-CA RA of all changes in the information featured in a certificate during the operational period of its certificate, or of any other fact that materially affects the validity of a certificate, such as changes to the TSP certification practices.

The COM-CA RA authorizes the issuance or the revocation of certificates at the request of a TSP duly authorized representative. In case of a proven TSP key compromise, the COM-CA shall immediately revoke the concerned TSP certificate.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The TSP dully authorized representative submits the certificate application as part of the overall process through which the TSP is authorized by the AECE PKI GB to setup its subscribing CA under the COM-CA.

4.1.2 Enrolment Process and Responsibilities

The COM-CA RA executes the necessary vetting checklist for TSPs and their applicant representatives. For any certificate application to the COM-CA, the identity of the applicant representative is verified by the COM-CA RA that verifies that all data provided in the certificate application are accurate.

The applicant representative will issue to the COM-CA RA its request for certificate issuance in a form of certificate application that includes a signed subscriber agreement. The COM-CA RA performs the necessary verification steps including:

- The identification of the TSP;
- Involve the PKI GB for reviewing the TSP CPS and ensuring the CPS complies with the relevant provisions of this CP/CPS and with the TSP CP;
- Description of the TSP purpose from the application;
- Required certificate profiles and the values of each attribute that should be present in the CA certificate;
- If deemed necessary, conduct a dry run of key ceremony with the TSP involving the respective test environments and test data;
- Verify the authority of the applicant representative through an attestation letter;
- Communication with the TSP to confirm all approvals are in place from the TSP top management. Such communication, depending on the circumstances, may include one, or more of the following: telephone, site visit, e-mail or registered mail delivery;
- Confirm with the AECE PKI GB that other pre-requisites related to establishing the TSP are processed by the PKI GB before the COM-CA RA can accept the certificate request.

The COM-CA RA securely stores the certificate application along with all supporting documentation for future reference.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Certificate applications for the COM-CA are received as part of an operational cycle agreed between the COM-CA RA and the applicant representative. The certificate application processing involves the identity verification of applicant representative through an in-person meeting. Other steps are executed by the COM-CA RA including the verification of the information provided in the certificate request form against the approved CPS versions.

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

- The existence of the applicant is verified using the official channels (e.g. chamber of commerce, Algerian Official Journal) which is expected to contain detailed information about the entity including its legal name and authorized official representative. The address of the requesting entity is also verified through an in-person visit from the COM-CA RA to the relevant address;
- the applicant representative’s identity is verified through an in-person meeting with the COM-CA RA that verifies the authority of the applicant representative through an attestation letter received;
- 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 applicant representation though a signed subscriber agreement;
- the CPS of the applicant is reviewed by the COM-CA RA;
- the cycle of mandated audit by the COM-CA RA successfully executed by the applicant.

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

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 PKI GB to process the certificate application, the AECE COM-CA RA shall agree with the applicant representative on a date for executing the TSP certification key ceremony.

In case the certificate application is rejected, the AECE COM-CA RA informs the TSP 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 certificate issuance for the Commercial TSP CA is executed in accordance with the AECE operational key ceremonies.

The COM-CA RA gathers all required parties at the AECE COM-CA primary facility to execute the TSP certificate generation. The pre-conditions for executing the ceremony are documented in clause 4.1 and 4.2. As part of the ceremony, the COM-CA RA performs final verification before processing the TSP certificate application. At a minimum, the following verification steps are performed:

- Identity verification of all attendees
- Validation of the format of the certificate request shall be in PKCS#10 format)
- Verification that the certificate request contains valid subscriber data (as agreed during the certificate application processing)

During the ceremony, PKI administrators in trusted roles direct commands for the COM-CA to perform a certificate signing operation.

Following the successful completion of the ceremony and the issuance of the TSP certificate, issued certificate contents are validated against the agreed TSP CA certificate format. The certificate is then handed over to the TSP representative. All parties that participated in the ceremony sign a ceremony report, including the TSP representative.

Further details on the certificate issuing process are documented in the related AECE key ceremony documentation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Following the successful completion of the ceremony and the issuance of the TSP certificate, the COM-CA RA edits the file contents in front of the TSP representative. The issued certificate contents are validated against the agreed TSP CA certificate format. The certificate is then handed over to the TSP representative.

The TSP PKI operations team will import the certificate by executing their own operational ceremony. If the CA certificate is successfully imported into the target TSP subscribing CA systems, the TSP PKI operations team publish the certificate on the TSP repository. The AECE COM-CA RA is notified on the successful import of the TSP CA certificate into the TSP target systems. This constitutes the formal acceptance by the TSP of the certificate issued by the COM-CA.

In case the certificate could not be processed successfully by the TSP target systems, the reasons for non-acceptance will be discussed with the AECE COM-CA RA and an investigation shall follow. If no measures can be agreed upon in order to obtain the certificate acceptance by the TSP target systems, the certificate shall be revoked by the COM-CA.

If it is possible to restart the ceremony in a way that the reason for non-acceptance is avoided, the ceremony will be repeated according to documented key exception ceremonies.

4.4.2 Publication of the Certificate by the CA

Following the acceptance of a certificate, AECE posts an 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, the subscriber's responsibilities include:

- Providing correct and up-to-date information to the COM-CA as part of its application.
- 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 CPS
- Protecting the CA private keys (and related secrets) from compromise, loss, disclosure, or otherwise unauthorized use of their private keys.
- Notifying the COM-CA RA immediately if any details in the certificate become invalid, or as a result of any compromise, loss, disclosure, 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 CPS for complementary details.

4.5.2 Relying party public key and certificate usage

A party relying on a certificate issued by the COM-CA shall:

- 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 COM-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 COM-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

The COM-CA does not allow certificate modification. In case the Subscriber wants to change the certified information, or has requested the revocation of their certificate due to circumstances mentioned in the previous paragraph, and wishes to be issued a new certificate, the Subscriber shall submit a full certificate application, as for initial enrolment.

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 PKI GB or by the TSP. The COM-CA RA shall ensure a Subordinate CA Certificate is revoked within a maximum of seven (7) days if one or more of the following events:

- The TSP requests revocation in writing;
- The TSP notifies the COM-CA RA that the original certificate request was not authorized and does not retroactively grant authorization;
- The PKI GB 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 PKI GB obtains evidence that the Certificate was misused;
- The PKI GB is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- The PKI GB determines that any of the information appearing in the Certificate is inaccurate or misleading;
- CA termination plan was triggered by the PKI GB or TSP so that COM-CA or Subordinate CA ceases operations for any reason and has not made arrangements as per the CA termination plan;
- The COM-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 COM-CA CP/CPS.

Whenever any of the above circumstances occur, the following process is executed by the AECE COM-CA RA:

- When the revocation request is triggered by the TSP, the AECE COM-CA RA performs the following steps:
    - the review and verification of the revocation request form received from the TSP authorized representative, this includes the verification of the identity of the requesters against the information available to the COM-CA RA (provided during the TSP enrolment);
    - communication with the TSP to provide reasonable assurances that the TSP official representative authorized the revocation operation and is aware of the circumstances that triggered the revocation request. Such communication, depending on the circumstances, may include one or more of the following: telephone, e-mail or registered mail delivery;
    - the organization of a face-to-face meeting involving relevant members from the TSP and the AECE PKI GB.
- When the AECE PKI GB triggers the TSP CA revocation after finding evidence of compromise, or suspected compromise of the TSP CA private key, the AECE COM-CA RA communicate with the TSP and shall ensure a Subordinate CA Certificate is revoked within a maximum of seven (7) days.

4.9.2 Who Can Request Revocation

The permanent revocation of a Certificate can be requested by:

- The Subscriber himself
- AECE at its own discretion (if for instance a compromise is known for this CA key)

Certification revocation requests from subscribers are only accepted if the subscriber is authorized and authenticated to request revocation for the specific certificate as described in section 4.9.1.

4.9.3 Procedure for Revocation Request

The PKI GB provides a continuous ability for subscribers to submit certificate revocation requests. Considering the criticality of the operation, the following procedure takes place:

- A meeting is organized by the PKI GB no later than twenty-four (24) hours after receiving the request from the subscriber.
- 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 PKI GB and the subscriber may request additional information/evidence from the technical teams which shall be provided within a maximum of forty-eight (48 hours).
- As soon as the revocation request relevance is confirmed through a formal communication between the PKI GB and the subscriber, the subscriber submits a formal revocation request to the COM-CA RA. This is approved by the PKI GB.
- The certificate revocation ceremony is planned and executed not later than seventy-two (72 hours) after the CA certificate revocation is authorized by the PKI GB. The revocation ceremony is witnessed by members in trusted role from the PKI GB and the subscriber. The outcome of the ceremony will be as follows:
    - The subscriber CA certificate is revoked with the right revocation reason on the COM-CA system;
    - A CRL is generated by the COM-CA and placed on the target public location within 24 hours maximum from the revocation;
    - The COM-CA and the subscribe shall 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 reports@aece.dz

The COM-CA discloses instructions related to certificate revocation and certificate problem reporting on its public repository. For any certificate problem report, the notifier is requested to include his contact details, suspected abuse and related domain name. The COM-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 PKI GB 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 PKI GB begins investigations within 24 hours from receipt. The PKI GB 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 filed 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 PKI GB.

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 COM-CA.

4.9.7 CRL Issuance Frequency

The COM-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 COM-CA is set to 184 days beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

Not stipulation.

4.9.9 Online Revocation/Status Checking Availability

The COM-CA offers an OCSP responder that conforms to RFC 6960 and whose certificate is signed by the COM-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 COM-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 COM-CA OCSP responder supports the HTTP GET method. The COM-CA OCSP Responders will not respond with a "good" status for a certificate that has not been issued.

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

The COM-CA OCSP responder that receive a request for status of a certificate that has not been issued, shall 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, will not respond with a "good" status for such Certificates.

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

4.9.12 Special Requirements — Key Compromise

If the PKI GB discovers, or has a reason to believe, that there has been a compromise of the COM-CA private key, this will be considered as a disaster scenario and the COM-CA Disaster Recovery and 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 be supported by the COM-CA.

4.9.14 Who Can Request Suspension

Not 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 shall is published by the COM-CA on a public repository which is available to relying parties through HTTP protocol queries.

The COM-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 shall be available 24 hours a day and 7 days a week, with an availability percentage of minimum 99 % over one year.

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

4.10.3 Optional Features

Not stipulation.

4.11 End of Subscription

Based on the TSP certificate revocation circumstances, the TSP termination plan may be triggered which implies the termination of the authorization granted from the AECE to the TSP to operate its certification services.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable. The COM-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 COM-CA operations team to perform the functions of key generation, certificate issuance, certificate revocation, audit, and archival.

The COM-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.

The PKI GB conducts an annual Risk Assessment on the COM-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 COM-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

COM-CA

The COM-CA PKI GB ensures that appropriate physical controls are implemented on the AECE-CA (hosting) premises for their activities. These physical controls are documented in internal documentation: "Logical/physical access control policies" and "Physical site requirements". These controls are enforced and verified regularly as follows:

- Regular internal audits performed by the AECE PKI GB audit function on the AECE PKI operations team
- Regular formal surveillance audits performed by the PMA on the AECE PKI operations and coordinated with the AECE PKI GB audit function

The AECE COM-CA premise 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 jointly by the AECE/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 AECE COM-CA systems.

5.1.2 Physical Access

The AECE COM-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 three 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 AECE COM-CA provides UPS and backup generators with enough capability to support the COM-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 COM-CA systems. All these systems ensure that the COM-CA equipment continuously operate within the manufacturers' range of operating temperatures and humidity.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The AECE PKI GB follows leading practices and applicable safety regulations in Algeria to ensure the COM-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 COM-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 COM-CA disaster recovery location.

5.1.7 Waste Disposal

All waste paper and storage media created within the secure facility shall be destroyed before discarding. Paper media shall be shredded using a cross-hatch shredder, and magnetic media shall be wiped by de-magnetization, or physically destroyed. HSMs and related key management devices shall be physically destroyed, or securely erased prior to disposal.

5.1.8 Offsite Backup

Full and incremental backups of the COM-CA online systems are taken regularly to provide enough recovery information when the recovery of the COM-CA systems 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 COM-CA operations team. Adequate back-up facilities ensure that backup copies are transferred to the disaster recovery location where it is 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 COM-CA Disaster Recovery plan.

Subscribing CAs

The TSP shall implement physical and environment controls for the facility hosting their CAs such that these controls at minimum, are in line with the COM-CA physical and environmental security controls listed above.

5.2 Procedural Controls

COM-CA

The AECE PKI GB ensures that the appropriate procedural controls are implemented for COM-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 AECE PKI GB 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 COM- CA, and to perform back-up, recovery and maintenance operations. Also authorized to add other users in the target COM-CA systems
- PKI system operation: Trusted roles authorized to execute the COM-CA operational cycle and is involved in critical operations such as subscribers' certification operations and COM-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 COM-CA operational ceremonies
- Security officers:
    - HSM administrator: Authorized to hold HSM activation data and secrets necessary for the HSM operation
    - Security operations: Authorized to collect and view the audit logs generated by the COM-CA systems as part of the continuous monitoring of the COM-CA systems
- Audit operation: Trusted role authorized to review the COM-CA systems audit logs as part of regular internal compliance audits

5.2.2 Number of Persons Required Per Task

The AECE PKI GB is responsible to ensure that the COM-CA operations team enforces segregation of duties for critical COM-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 COM-CA operations manager. These forms are used as part of the regular internal audits performed by the PMA audit and compliance function on the COM-CA operations.

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

The AECE PKI GB ensures that all operational activity performed by COM-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 AECE PKI GB confirms the identity and history of the employee by carrying out background and security checks.
- When instructed through the internal PKI GB processes, the facility operations team issues an access card to each staff who needs to physically access equipment located in the secure enclave.
- COM-CA dedicated staff (system administrators) issue the necessary ICT system credentials for COM-CA staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

AECE 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)

Subscribing CAs

The TSP shall implement procedural controls that at minimum, are in line with the COM-CA procedural controls listed above.

5.3 Personnel Controls

COM-CA

The PKI GB mandates the implementation of security controls for the duties and roles of the staff members in charge of the COM-CA activities.

The COM-CA‘s personnel security controls include the following:

5.3.1 Qualifications, Experience and Clearance Requirements

All COM-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, which are given to the AECE PKI GB. While performing any critical operation on the COM-CA systems, trusted roles are to be held by an Algerian national only.

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

The PKI GB 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 COM CA operations. This training is regularly updated and delivered on a yearly basis to COM-CA personnel.

The training curriculum is delivered by a mix of COM-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 COM-CA services. In particular, the training curriculum covers basic and advanced topics necessary for the COM-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 PKI GB 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 COM-CA personnel. The training content is reviewed and amended on a yearly basis to reflect the latest leading practices and COM-CA configuration changes.

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

For the purpose of maintaining accountability on COM-CA personnel, the PKI GB shall sanction 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 AECE 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 PKI GB 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 AECE PKI GB shall document all training material and make it available to COM-CA personnel. The PKI GB also ensures that key documentation related to COM-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.

Subscribing CAs

The TSP shall implement personnel security controls that at minimum, are in line with the COM-CA procedural controls listed above.

5.4 Audit Logging Procedures

COM-CA

The COM-CA systems operated by the COM-CA operations team shall maintain an audit trail for material events and operations executed on the COM-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 shall be generated and preserved. These logs shall be reviewed by the COM-CA security monitoring team, and are also reviewed as part of the regular internal audits performed by the AECE PKI GB audit function on COM-CA operations.

The AECE PKI GB 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 COM-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 COM-CA operations team and may be made available during compliance audits.

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

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

The AECE PKI GB 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 AECE PKI GB:

- COM-CA application and security audit logs shall be reviewed by the security operations team on a 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 COM-CA systems with an objective to continuously validate the on-going physical and logical access policies
- Every six (6) months, the AECE PKI GB audit and compliance function executes an internal audit of the COM-CA operations. Samples of the audit logs produced since the last audit cycle shall be requested by the PKI GB 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 PKI GB ensures that the audit logs are maintained and retained onsite for a period not less than six (6) months. These audit logs are also replicated and retained in the disaster recovery location for the same period.

Past the six (6) months period, the audit logs are archived for a period not less than seven (7) years. These may be made available to the COM-CA 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 COM-CA 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 COM-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 COM-CA operations personnel.

5.4.5 Audit Log Backup Procedures

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

- Backup media are stored locally in the COM-CA 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 COM-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 audit collection system, no notice is required to be given to the individual, organization, device or application that caused the event.

5.4.8 Vulnerability Assessments

The COM-CA systems and infrastructure shall be subject to regular security assessment as follows:

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

The outcome of the regular assessments and identified issues shall be made available to the COM-CA upper PKI operations management, who shall be responsible to organize and oversee the execution of the remediations by the respective teams.

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

The AECE PKI GB 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 COM-CA higher PKI operational management will develop and present a security plan to the PKI GB seeking the necessary approvals to proceed with the remediation implementation.

Subscribing CAs

The TSP shall implement audit and logging security controls that at minimum, are in line with the COM-CA controls listed above.

5.5 Records Archival

COM-CA

The COM-CA operations ensure that records are archived for a period not less than seven (7) years. The archived records shall provide sufficient details and information on the COM-CA operations over that period. The archived information shall include at minimum:

- All issued certificates by the COM-CA in a way such that expired certificates would be retained in the archive for a period of Seven (7) years after expiration
- Audit logs of COM-CA certificate lifecycle operations (including certificate issuance and revocation)
- All CRLs issued by the COM-CA

Audit logs are archived in a retrievable format. Procedural and technical controls shall be enforced by the COM-CA operations team to protect the integrity and prevent data loss of the storage media holding the archived audit logs.

5.5.1 Types of records archived

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

- PKI transaction logs for the COM-CA including Certificate lifecycle management (certificate creation and certificate revocation);
- OCSP responder events log;
- All CRLs generated by the COM-CA;
- All versions of this CP/CPS and subscriber agreements;

- Key ceremony documentation and related verification information;

5.5.2 Retention period for archive

As stated in clause 5.5.

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 logs are protected by a combination of physical, procedural and technical security controls as follows. Archived logs are securely maintained using the access control mechanisms enforced by the COM-CA support systems. These policies ensure that only read-access is granted to personnel having access to all archived logs 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 COM-CA. The COM-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 COM-CA systems is synchronized with the time source of a GPS clock. Further, the COM-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 shall be allowed to access archived material. The COM-CA operations team use the COM-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.

Subscribing CAs

The TSP shall implement audit record archival security controls that at minimum, are in line with the COM-CA controls listed above.

5.6 Key Changeover

To minimize impact of key compromise, the COM-CA key shall be changed with a frequency that ensures the COM-CA shall have a validity period greater than the maximum lifetime of Subscriber certificate after the latest Subscriber certificate issuance.

Refer to section 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

COM-CA

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

The PKI GB 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.

Subscribing CAs

The TSP shall implement incident and compromise handling procedures that at minimum, are in line with the COM-CA arrangements listed above in addition to the relevant requirements indorsed by the national TSP CP.

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

COM-CA

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

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

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

Subscribing CAs

The TSP shall implement controls to protect their CA systems from software/resources/data corruption. These controls at minimum, are in line with the COM-CA arrangements listed above in addition to the relevant requirements indorsed by the national TSP CP.

5.7.3 Entity private key compromise procedures

COM-CA

Compromise of the COM-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 AECE disaster recovery and business continuity plan.

Considering the criticality of such compromise situation and its impact on the Algeria national PKI, the PMA and the PKI GB hold an exceptional meeting. Refer to sections 4.9.1 and 4.9.3 for further details.

Subscribing CAs

The TSP shall enforce private key compromise procedures related to their CAs.

5.7.4 Business continuity capabilities after a disaster

COM-CA

In case of a disaster, corrupted servers, software or data, the COM-CA disaster recovery and business continuity plan is triggered in order to restore the minimum COM-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 COM-CA certificates are published
- COM-CA OCSP service

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

The COM-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 COM-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 COM-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

Subscribing CAs

The TSP shall implement business continuity capabilities (after disaster) as part of their operations.

5.8 CA or RA Termination

COM-CA

Refer to clauses 4.9 and 5.7 of this CP/CPS for COM-CA key compromise and revocation.

Subscribing CAs

The TSP shall have a Termination Plan duly tested and ready to be triggered when required.

6 Technical Security Controls

This clause defines the security measures the PKI GB 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 COM-CA shall implement and document key generation procedures in accordance with this CP/CPS.

6.1.1 CA Private Key Pair Generation

COM-CA

The COM-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 PKI GB. The ceremony requires HSMs that meet the requirements of FIPS 140-2 Level 3, and a dedicated machine to be setup by authorized COM-CA personnel only. The detailed key ceremony activities are documented in the COM-CA key ceremony procedure and related ceremony log. The ceremony involves the execution of technical procedures through which the COM-CA personnel setup the COM-CA software and trigger the COM-CA key pair generation and Certificate Signing Request (CSR) creation through the COM-CA HSM. The COM-CA CSR is signed by the National Root CA and the COM-CA certificate is imported through the COM-CA software to complete the COM-CA key ceremony.The trusted personnel involved in the COM-CA key generation ceremony select their own secrets and HSM activation data is then generated. All COM-CA private key material, secrets and activation data is maintained in tamper evident envelopes during the entire lifecycle of the COM-CA private key.

The COM-CA Key Generation Ceremony is witnessed by a WebTrust qualified auditor. The activities performed in each COM-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 COM-CA backup and archive procedures.

Subscribing CAs

The AECE PKI GB oversees the establishment of the Commercial TSP and approves their respective ceremonies after the completion of several verifications including the successful completion of a surveillance audit on the TSP operations. The key generation ceremony for the TSP CA is witnessed by the AECE PKI GB audit function. The security measures that are in place for the key generation of AECE issuing CAs shall be described in their respective CPS.

6.1.2 Private key delivery to subscriber

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

6.1.3 Public key delivery to certificate issuer

Subscribing CAs

The TSP obtains its public key through a certificate request. The request is processed as part of COM-CA ceremonies which result in the generation of the TSP CA certificate, which is handed over to the TSP representative. The public key is then imported into the target TSP CA systems. Refer to clauses 4.3, 4.4 and 6.1.1 of this CP/CPS for further details.

6.1.4 CA public key delivery to relying parties

The COM-CA operations team ensures the COM-CA certificate and the Subordinate CA certificates are published on the AECE public repository.

6.1.5 Key sizes

COM-CA

The minimum size for the COM-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

COM-CA

The COM-CA public Key module generation is done with HSM devices that that conforms to FIPS 186-2 for random generation and primality checks. The COM-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)

COM-CA

Private Keys corresponding to the COM-CA Certificates shall not be used to sign Certificates except in the following cases:

- Certificates for Subordinate CAs;
- And certificates for COM-CA OCSP responder.

Subscribing CAs

The Subscribing CAs uses private signing keys only for signing CRLs and applicant certification services in accordance with the intended use of each of these keys. Other usages are restricted. Certificates issued to subscribing CA shall always contain key usage bit string in accordance with RFC 5280.

- keyCertSign
- cRLSign

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The COM-CA operations team implements physical and logical safeguards to prevent unauthorized certificate issuance. The COM-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 COM-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

COM-CA

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

Subscribing CAs

COM-CA provisions shall apply to subscribing CAs that shall use certified/validated for FIPS 140-2 Level 3 or equivalent levels of security certification.

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

COM-CA

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

COM-CA personnel are assigned to the trusted roles by the AECE PKI GB ensuring segregation of duties and enforcing the principles of multi control and split knowledge. Multi-person control of the COM-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 PKI GB staff, to activate or re-activate the COM-CA private key. The PKI GB 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 – Commercial TSP

The TSP shall enforce private key shared control procedures to their CAs.

6.2.3 Private key escrow

COM-CA

Private keys of the COM-CA are not escrowed. Dedicated backup and restore procedures of the COM-CA private key are implemented by the AECE.

Subscribing CAs

Private keys of the subscribing CAs may not be escrowed.

6.2.4 Private key backup

COM-CA

The COM-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 COM-CA key generation ceremonies. The COM-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 COM-CA private keys that are physically transported from the primary facility to the DR one using a dedicated HSM handling and key handling procedure part of the overall COM-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 COM-CA private key backup.

6.2.5 Private key archival

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

6.2.6 Private key transfer into or from a cryptographic module

COM-CA

The COM-CA uses FIPS 140-2 Level 3 certified/validated HSMs for the primary and disaster recovery facilities. COM-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 with 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 COM-CA private key has been compromised and potentially communicated to an unauthorized person or organization, then the PKI GB 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 COM-CA private key transfer to/from cryptographic modules, shall apply to subscribing CAs private key transfer.

6.2.7 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.

6.2.8 Method of activating private key

COM-CA

The COM-CA private key is activated inside the HSM as part of audited key ceremonies attended by several trusted personnel and relevant PKI GB 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 COM-CA key remain active only for the duration of the activity requiring the COM-CA activation (e.g. certification, CRL generation). The details of COM-CA private keys activation are documented in the COM-CA key ceremony documentation.

Subscribing CAs

TSPs activate their own private keys. The same security measures and methods to activate COM-CA private keys shall apply to activating the private keys of TSP CA private keys.

6.2.9 Method of deactivating private key

COM-CA

The HSMs used for the COM-CA key ceremony are deactivated at the end of the ceremony which prevents any further use of the COM-CA private keys. This activity applies to the principles of dual control and split knowledge, and shall always be witnessed by the relevant personnel (PKI GB, 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

Similar provisions, related to COM-CA private key deactivation, shall apply to the TSP CA private key deactivation.

6.2.10 Method of destroying private key

COM-CA

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

The COM-CA keys are destroyed by permanently removing it from any hardware module the keys are stored on. The hardware module will be then reset or returned to its factory state.

The COM-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 COM-CA private key destruction, shall apply to the TSP subscribing CAs private key destruction.

6.2.11 Cryptographic Module Rating

COM-CA

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

Subscribing CAs

The subscribing CAs cryptographic modules shall be certified/validated at minimum 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 COM-CA certificate shall have a validity period at least greater than the last Subscriber certificate it issued, augmented with a grace period that takes into account the COM-CA key ceremony procedure. The same rule shall be enforced by the subscribing CA for the certificates it issues.

COM-CA

The COM-CA certificates shall be valid for seventeen (17) years, with a key usage period for signing Subscriber certificates of five (5) years. After five (5) years, the CA certificate will continue to be used for signing CRL but does not issue any new subscriber certificates.

Subscribing CAs

In the case of a subordinate (non-issuing) TSP CA, the provisions of this CP/CPS suggest TSP CA certificates valid for eight (8) years, with a key usage period of three (3) years.

In the case of an issuing CA for the TSP (issuing certificates for end-users), the provisions of this CP/CPS suggest TSP CA certificates valid for five (5) years, with a key usage period of two (2) years.

6.4 Activation Data

6.4.1 Activation data generation and installation

COM-CA

The COM-CA private key and related HSM activation is generated during the COM-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 COM-CA activation data generation and installation.

6.4.2 Activation data protection

COM-CA

The COM-CA private key and related HSM activation data is generated during the COM-CA private key generation ceremony. The protection mechanisms applied on the COM-CA keys apply also to the HSM and keys activation data. 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 protection shall be subject to the same security controls as the COM-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

COM-CA

The COM-CA operations team is subject to the security controls documented in the COM-CA policy manual. The COM-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 COM-CA systems and end-point protection;
- Backup and recovery mechanisms for COM-CA operations;
- Hardening of COM-CA servers' operating system according to leading practices and vendor recommendations;
- In-depth network security architecture including perimeter and internal firewalls, web application firewalls, including intrusion detection systems;
- Proactive patch management as part of the COM-CA operational processes;
- The COM-CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

The AECE PKI GB organizes regular (at minimum twice a year) internal audit to monitor the COM-CA operations against the target security controls. The COM-CA is also subject to regular surveillance audits from the PMA.

Subscribing CAs

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

6.5.2 Computer Security Rating

The COM-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

6.6.1 System Development Controls

COM-CA

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 COM-CA trusted personnel are involved to implement the required COM-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 COM-CA operations team.

All COM-CA hardware and software platforms are hardened using industry best practices and vendor recommendations.

Subscribing CAs

The subscribing CA's shall be subject to the same system development controls as the COM-CA.

6.6.2 Security Management Controls

COM-CA

The hardware and software used to set up the COM-CA shall be dedicated to performing only CA-related tasks. There shall be 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 COM-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 COM-CA usage.

Refer to clause 6.6.1 for further details.

Subscribing CAs

The subscribing CA's shall be subject to the same security management controls as the COM-CA.

6.6.3 Life-Cycle Security Controls

Refer to 6.5.1.

6.7 Network security controls

COM-CA

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

The COM-CA repository and OCSP responder are online systems supporting the COM-CA operations and enabling service provision to relying parties, in compliance with the provisions of this CP/CPS. An 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 COM-CA systems. These controls and technologies limit the services allowed to and from the COM-CA online services.

The AECE PKI GB ensures regular vulnerability testing is conducted on the COM-CA online services. The AECE PKI GB also ensures that at least once a year, penetration testing is conducted on the COM-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 COM-CA network.

6.8 Time-stamping

COM-CA

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

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

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

Subscribing CAs

The CA servers' internal clock shall be synchronized using the NTP service.

7 Certificates and CRL Profiles

7.1 Certificate Profile

Subscribing CA certificate profile – TSP intermediate CA (non-issuing)

Commercial TSP Intermediate CA Certificate Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M	S		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	Commercial CA's Signature	Commercial 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	S		
CountryName				DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

OrganizationName				AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName				Commercial 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 + **[96]** Months	Suggested validity to cope with key changeover rules
Subject	False	M	D		
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	Allocated as per certificate request	UTF8 encoded
OrganizationName		M	D	Allocated as per certificate request	UTF8 encoded
CommonName		M	D	Allocated as per certificate request	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	O			
	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	D	http://ocsp.pki.aece.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	D	http://pki.aece.dz/repository/cert/commercial_ca.p7b	Commercial CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	D	http://pki.aece.dz/repository/crl/commercial_ca.crl	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey
Policy Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
CertificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.12.3.3.1.1	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	https://pki.aece.dz/repository/cps	
BasicConstraints		True	M			
	CA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		M	S	1	

Subscribing CA certificate profile – TSP issuing CA

Commercial TSP Issuing CA Certificate Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M	S		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	Intermediate CA Signature	Issuing CA 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	S		
CountryName				DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName				AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE or *<OrganizationName of the Commercial Entity level 1 CA>*	UTF8 encoded
OrganizationUnitName		O	D	Not present if the issuer is Commercial CA, otherwise it could be the	

				OrganizationUnitName of the Commercial Entity level 1 CA subject	
CommonName				Commercial CA or *<CommonName of TSP intermediate 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 + **[60]** Months	Suggested validity to cope with key changeover rules
Subject	False	M	D		
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	Allocated as per certificate request	UTF8 encoded
OrganizationName		M	D	Allocated as per certificate request	UTF8 encoded
CommonName		M	D	Allocated as per certificate request	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	O			
	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	D	http://ocsp.pki.aece.dz or *<HTTP URL FOR Intermediate CA's OCSP SERVICE>*	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	D	http://pki.aece.dz/repository/cert/commercial_ca.p7b or *<HTTP URL FOR Intermediate CA's PKCS7 FILE>*	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	D	http://pki.aece.dz/repository/crl/commercial_ca.crl or *<HTTP URL pointing to CRL issued by Intermediate CA>*	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey
Policy Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
ExtendedKeyUsage		False	O			MUST be present if the CA is

					technically constrained
	serverAuthentication		O	S	True	
	clientAuthentication		O	S	True	
	emailProtection		O	S	True	
	codeSigning		O	S	True	
	id-kp-OCSPSigning		O	S	True	
NameConstraints		True	O			Could be present if the serverAuthentication presents in the EKU
	permittedSubtrees		M	S	<Allowed values for the TLS Server domain names e.g. “host.example.dz" for a host and ".example.dz" for a wildcard domain name>	Applies to both Subject DN and Subject Alternative Names.
CertificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.12.3.3.1.1 or *<OID of the Commercial TSP intermediate CA CPS>*	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	https://pki.aece.dz/repository/cps or *<URL location of the TSP intermediate CA CPS >*	
BasicConstraints		True	M			
	CA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		M	S	0	

7.1.1 Version number(s)

X.509 v3 is supported and used for all certificates related to the COM-CA (see table 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 table 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 certificate profiles (see table in clause 7.1).

7.1.5 Name constraints

Name constraints are supported as per RFC 5280.

7.1.6 Certificate policy object identifier

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

OIDs used are provided in the certificates profiles as described in the table in clause 7.1.

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 certificates profiles as described in the table 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 COM-CA supports CRLs compliant with:

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

The COM-CA's CRL is as follows:

CRL Profile						
Field		CE[2]	O/M[3]	CO[4]	Value	Comment
CertificateList			M			
TBSCertificate						
Signature		False	M			
	AlgorithmIdentifier			S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
	SignatureValue			D	CA's Signature.	CA's signature value
TbSCertList		False				
Version		False	M			

	Version			S	1	Version 2
Signature		False	M			
	AlgorithmIdentifier			S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer		False	M	S		
CountryName					DZ	
OrganizationName					AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE	
CommonName					Commercial CA	
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	thisUpdate			D	<creation time>	
	NextUpdate			D	<Creation time> + **[184]** days	
RevokedCertificates		False	O			
Certificate						
	CertificateSerialNumber			D	Serial of the revoked certificates	
	revocationDate			D	Date when revocation was processed by the CA	UTC time of revocation
	crlEntryExtension	False	O			
	CRLReason			S	As per RFC 5280	Identifies the reason for the certificate revocation
	Invalidity Date			S	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		D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey of the CA public key
	CRL Number	False				Sequential CRL Number
AuthorityInfoAccess		False	O			
	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	D	http://pki.aece.dz/repository/cert/commercial_ca.p7b	Commercial CA Certificate/Chain download URL over HTTP

7.2.1 Version number(s)

The COM-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 COM-CA OCSP response signing certificate profile is as follows:

OCSP Response Signing 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	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	S	<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName					DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName					AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName					Commercial 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	D		
CountryName			M		DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName			M		AUTORITE ECONOMIQUE DE	UTF8 encoded

				CERTIFICATION ELECTRONIQUE	
stateOrProvinceName		M	S	Algiers	UTF8 encoded.
CommonName		M		Commercial 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
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
nonRepudiation		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.3.1.1	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	https://pki.aece.dz/repository/cps	

7.3.1 Version number(s)

The COM-CA OCSP responders conform to RFC 6960.

7.3.2 OCSP extensions

No stipulations.

8 Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

The AECE PKI GB ensures that the COM-CA and the TSPs operations are subject to regular internal audits. These audits are planned and executed, at a minimum, twice a year by the PKI GB audit function. This internal audit is part of the PKI GB operational cycle, and remediation for the audit findings is implemented by the CA operations team in a timely manner.

External audits:

COM-CA

External audits are planned and executed by an independent WebTrust practitioner according to the WebTrust audit scheme. These are organized on a yearly basis by the PMA and apply for the COM-CA.

Subscribing CAs

External audits are planned and executed by an independent WebTrust practitioner according to the WebTrust audit scheme. These are organized on a yearly basis by the AECE PKI GB and apply for the TSPs operating unconstrained CAs.

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 AECE PKI GB audit function is independent of the COM-CA operations team.

External auditors are independent third party WebTrust practitioners.

8.4 Topics covered by assessment

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

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities

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 AECE PKI GB.

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 PKI GB. 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 PKI GB, and shall not be disclosed to non-authorised third parties.

External audits are published on the COM-CA repository.

8.7 Self-audits

The PKI GB, 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 every 6 months. 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

Certification services offered to TSPs are subject to payment, the amount of which is fixed by regulation.

The tariff conditions in force for the certificate application or renewal (re-key) are available from the AECE.

9.1.2 Certificate Access Fees

AECE does not charge for access to issued certificates.

9.1.3 Revocation or Status Information Access Fees

AECE does not charge a certificate revocation fee or a fee for checking the validity status of an issued certificate using a CRL or via OCSP.

9.1.4 Fees for Other Services

AECE may charge for other services depending on business needs and internal approval.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance coverage

AECE contract all the insurance, under the current regulations, necessary to cover the risks related to its missions.

It is the sole responsibility of TSPs, under the current regulations, to ensure a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other assets

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

9.2.3 Insurance or warranty coverage for end-entities

Not Applicable

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

- Subscriber's personal information that are not part of certificates or CRLs issued by the COM-CA
- Correspondence between the TSP and the COM-CA RA during the certificate management processing (including the collected subscribers data)
- Contractual agreements between the AECE and its suppliers
- AECE 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 AECE repository.

9.3.3 Responsibility to protect confidential information

The AECE 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 AECE observes personal data privacy rules and privacy rules as specified in the present CP/CPS. The AECE implements these provisions through the COM-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 AECE 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 AECE to subscribers (TSPs) except for information about themselves and only covered by the contractual agreement between the AECE and the TSPs.

The AECE will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the AECE releases private information, AECE will ensue through reasonable means that this information is not be 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 communications channels with the AECE shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the COM CA systems. This shall include:

- The communications between the COM-CA RA systems and the subscribers (TSPs);
- 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 AECE employees, suppliers and contractors handle personal information in strict confidence under the AECE 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 AECE ensure that collected personal information is used for the purpose of certificate life cycle management only as consented by the subscribers (TSPs).

Unless otherwise stated in this CP/CPS, the AECE 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 AECE 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 AECE PKI GB owns and reserves all intellectual property rights associated with the COM-CA databases, repository, the COM-CAs digital certificates and any other publication originating from the PKI GB, including this CP/CPS.

The COM-CA uses software from third-party PKI products suppliers. This software remains the intellectual property of the product suppliers, and its usage by the COM-CA bound by license agreements between the PKI GB and these suppliers.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

The COM-CA is responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with the requirements of this CP/CPS, and for any related liabilities and indemnification obligations of the Subordinate CA.

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

The AECE warrants that each Applicant 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 AECE 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 AECE requires, as part of the Subscriber Agreement that the Applicant make the commitments and warranties in this section for the benefit of the Certificate Beneficiaries. Prior to the issuance of a Certificate, the AECE SHALL obtain, for its express benefit and the Certificate Beneficiaries the Applicant's agreement to the Subscriber Agreement with the AECE.

The AECE implements a process to ensure that each Subscriber Agreement 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 AECE, both in the certificate request and as otherwise requested by AECE in connection with the issuance of the Certificate(s) to be supplied by the COM-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 AECE instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the AECE 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 COM-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 COM-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 AECE 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 COM-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 COM-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 AECE PKI GB and related to the COM-CA services

9.8 Limitations of Liability

Limitations on Liability:

- The AECE will not incur any liability to TSPs or their Subscribers to the extent that such liability results from their negligence, fraud or wilful misconduct;
- The AECE 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. TSPs will immediately indemnify the AECE from and against any such liability and costs and claims arising there from;
- The AECE 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;
- TSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by AECE;
- TSP to compensate a Relying Party which incurs a loss as a result of the TSP’s breach of Subscriber’s agreement;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- The AECE denies any financial or any other kind of responsibility for damages or impairments resulting from the COM-CA operation.

9.9 Indemnities

This 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 AECE PKI GB and shall remain in force until amendments are published on the PKI GB repository and relevant communication towards TSPs.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The PKI GB coordinates communications towards the TSPs 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 TSPs to the PKI GB. 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 AECE PKI GB reserves the right to change this CP/CPS as and when need. The PKI GB 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 COM-CA repository, the newer version of the CP/CPS becomes effective. The older versions of this document are archived on the COM-CA repository. The PKI GB coordinates communication towards the TSPs 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 PKI GB shall coordinate proper communication to TSPs.

9.13 Dispute Resolution Provisions

All disputes associated with the provisions of this CP/CPS and the COM-CA services, shall be first addressed to AECE. If mediation by the AECE is not successful, then the dispute shall be addressed to the PMA then further to be submitted to competent territorial courts if the PMA mediation was not successful.

9.14 Governing Law

This CP/CPS shall in all respects be governed in accordance with the laws of the people's democratic republic of Algeria.

9.15 Compliance with applicable law

This CP/CPS and provision of COM-CA certification services are compliant to relevant and applicable laws of the people's democratic republic of Algeria. In particular:

- law 15-04 of Rabie Ethani 11t^{h}, 1436 corresponding to February 1st, 2015 fixing "*les règles générales relatives à la signature et à la certification électroniques*" and regulatory texts taken for its application

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 COM-CA CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of the AECE.

9.16.3 Severability

If any provision of this CP/CPS is determined to be invalid or unenforceable, the other sections shall remain in effect until this CP/CPS is updated.
In the event of a conflict between the Baseline Requirements and any regulation in Algeria, the AECE 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 AECE 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 AECE. The AECE will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS. Any modification to the AECE 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 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 AECE shall not be liable for any failure or delay in their performance under the provisions of this CP/CPS to any causes that are irresistible, unforeseeable, insurmountable event beyond its reasonable control.

9.17 Other Provisions

Not applicable.