PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

GOVERNMENT ELECTRONIC CERTIFICATION AUTHORITY

Government Certification Authority CP/CPS

Version 2.4

17 April 2024

PUBLIC

Version History

Version	Date	Change Description
V0.1	18/03/2019	Document preparation
V0.2	17/04/2019	Proofreading & formatting
V0.3	29/04/2019	Complete draft for customer
V0.4	30/09/2019	Typos, feedback from customer and further details on government TSP.
V0.5	25/10/2019	Additional feedback from customer and further details on government TSP.
V0.6	05/12/2019	Addressing additional feedback from customer. Version ready for final review
V0.7	29//01/2020	Addressing initial comments from the WebTrust auditor
V0.8	22/02/2020	Corrected few typos and changed CA DNs as per final decisions from PKI management
V1.0	23/03/2020	Added final URLs and corrected few typos
V1.1	25/10/2020	Applying final comments from the WebTrust auditor
V1.2	01/10/2021	Yearly Review
V2.0	10/02/2022	• Certificate profiles updated following the new Baseline requirements related to adding Extended Key Usage (EKU) extensions to all Subordinate CAs certificates under the National Root CA. • Reflect the new PKI Hierarchy of Government Domain • Changes to accommodate to: o Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.8.0 which is linked to WebTrust for SSL BR v2.6 o Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates v2.7 which is linked to WebTrust for CS BR v2.7
V2.1	29/05/2023	• Yearly review and sanity check • Amendments to code signing CA certificate profile following the SSL self-assessment report
V2.2	13/08/2023	• Update OCSP certificate profiles passed in baseline requirements version 2.0.0 • Sanity check
V2.3	26/11/2023	• Updates to the section related to methods of destroying private key. • Update the OCSP certificate Profile following the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 2.0.1
V2.4	17/04/2024	• Extend CRLs validity period to 12 months sections 2.3, 4.9.7, 4.9.10 and 7.2 • Adjustments in table format of all profiles in section 7 • General clean up and minor corrections

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
2.4	17/04/2024	AGCE	AGCE (PKI GB)	ANCE (PMA)

Table of Contents

1 Introduction

The present Certificate Policy and Certification Practice Statement (hereinafter, CP/CPS) applies to the certification services of the government CAs established and operated by the Government Authority for Electronic Certification (hereinafter, AGCE)

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.

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 AGCE with regard to all services available during the lifetime of certificates issued by the Government CAs.

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 Government CAs can be obtained from the AGCE PKI Governance Board (AGCE 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 National Root Certification Authority of Algeria (hereinafter, NR-CA). With this National PKI, the Algerian Government aims to provide a framework to facilitate the establishment of Trust Service Providers (TSP) offering digital certification and trust services to government and non-government entities.

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

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

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

- **Government CAs:**

  Five (05) Intermediate CAs certified by the Root CA, namely: **Government CA, Government TLS CA, Government CS CA, Government SMIME CA, Government TS CA.**

  Each Government CA certifies one issuing CA to cover particular extended Key usages:

  - **Corporate CA:** will issue Digital Signature and Authentication certificates to natural persons (government employees) and legal persons (government entities).
  - **OV TLS Server CA:** will issue organization validated Server Authentication certificates to non-natural entities such as servers and VPN device certificates. It will also issue Client Authentication certificates to non-natural organization end entities (devices).

- **SMIME CA:** will issue email protection (SMIME) certificates to natural persons (government employees).
- **Code Signing CA:** will issue code signing certificates to legal persons (government entities).
- **Trust services CA:** will issue timestamping certificates for AGCE and Government TSPs operating Timestamping services. It will also issue signing certificates for digital signature verification service operated by governmental TSPs.

In addition to the above issuing CAs, there is a scenario where a Governmental TSPs can establish their own certification services under the Government CA. The Government CA will certify an issuing CA operated by the TSP. This CA shall be technically constrained where the CA certificate (issued by the Government CA) will be populated with an extended key usage extension to limit the scope within which the issuing CA from the TSP may issue end-user certificates; The Government CAs only issue CA certificates to TSPs that are under the control of government entities. AGCE is responsible for the supervision and authorization of the TSP that shall successfully complete an authorisation process.

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

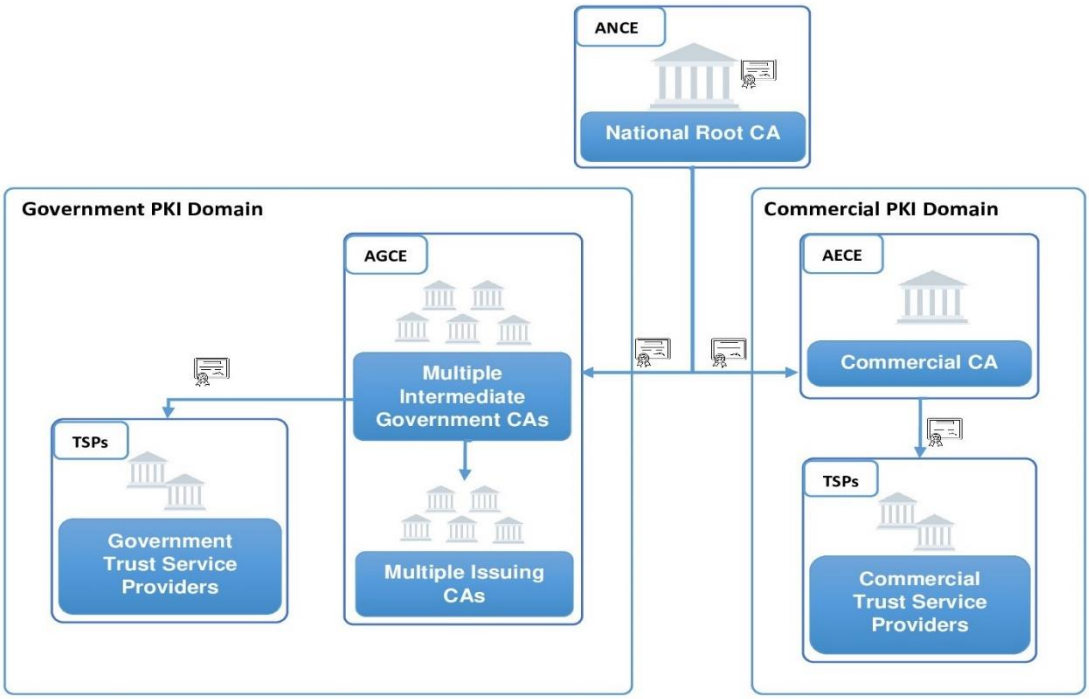

Figure 1: The Algerian National PKI hierarchy

1.2 Document Name and Identification

This document is titled "**Government Certification Authority CP/CPS**" and is referenced in related documents as [**AGCE GOV-CA CP/CPS**].

AGCE will also use the **OID 2.16.12.3.2.1.1** to identify this document.

1.3 PKI Participants

Several parties make up the participants of AGCE PKI. The parties mentioned hereunder including the AGCE CAs, the AGCE RAs, subscribers and relying parties are collectively called PKI participants.

1.3.1 Certification Authorities

The Government CAs are Certification Authorities operated by AGCE from dedicated facilities located in Algeria. AGCE issues Government CAs' 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.

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

- PKI Governance Board: Operating as the governance function for the AGCE PKI. It groups the necessary functions for this purpose including the policy, compliance and design functions. The PKI Governance Board (hereinafter, PKI GB) provides strategic direction and continuously supervises the AGCE operations team. The AGCE PKI GB operating cycle includes interactions with the PMA which is responsible for overseeing the operations of the Government CAs and other trust services operated by the AGCE) through regular supervision audits conducted by the PMA audit and compliance function;
- PKI operations: This technical operations structure is responsible for operating the trust services implemented by AGCE, including the Government CAs and issuing CAs certified by the Government CAs. It falls under the management and supervision of the PKI GB.

The Government CAs are 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 CP/CPS which the Government Certification Authority 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 the AGCE and other TSPs operating and approved under the Algerian PKI framework.

1.3.2 Registration Authorities

AGCE operates the RA function of the Government CAs. The RA function falls within the PKI operations structure and responsible for processing certificate management requests of the CAs (TSPs) under the Government CAs. When a TSP requests for the creation of a CA certificate under the Government CAs, 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 the subordinate CAs certified by the Government CAs.

The AGCE issuing CAs are among the subscribing CAs governed by this CP/CPS. The subscribers:

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

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 Government CA using the AGCE Certificate Validity Status Service (e.g. CRL, webpage, OCSP), prior to relying on information featured in said certificate.

The AGCE CAs certificates are published on the AGCE 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 Government CAs that includes the ones stated hereunder.

1.4.1 Appropriate certificate uses

The certificates issued by the Government CAs can be used to:

- 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.

1.4.2 Prohibited certificate uses

Certain limitations apply to the usage of certificates issued by the Government CAs as stated in this CP/CPS:

- 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 AGCE.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The AGCE 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 "**Algeria Root CA CP/CPS**" (**OID 2.16.12.3.1.1.1**).

The AGCE 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 "**Algeria Root CA CP/CPS**";
- Publishing this CP/CPS and its revisions.

1.5.2 Contact person

The AGCE can be contacted at the following address:

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

The AGCE 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 Government CAs by sending an email to Certification.Problem@agce.dz.

The AGCE 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 AGCE 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 AGCE 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 AGCE PKI GB as well as the PMA formally approves the new 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 this CP/CPS. The source is cited where relevant.

Applicant — The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.

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

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

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 Government CAs and Subordinate CAs.

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

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

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

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

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

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

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

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

Issuing CA — In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA. In the context of this CPS the issuing CAs refer to the AGCE subscribing CAs.

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 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.

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

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

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

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

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

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

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

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

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

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
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 Confiance 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 refers to the following:

- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

- RFC5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 6960 — X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- Webtrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates
- CA/B Forum Network and Certificate System Security Requirements;
- Algerian Law 15-04 on *« Digital Signature and Electronic certification »* (*Loi n° 15-04 du 01 Février 2015, fixant les règles générales relatives à la signature et à la certification électroniques)*
- Decree 135 (*AGCE décret exécutif N°16-135 fr*)
- Decree 134 (*ANCE décret exécutif N°16-134 fr*)
- Law 18-07 on the protection of individuals with regard to the processing of personal data

2 Publication and Repository Responsibilities

2.1 Repositories

AGCE maintains an online repository of documents where it makes certain disclosures about its CAs' practices, procedures and the content of some of its policies. Published information include:

- This CP/CPS;
- TSP CP;
- PKI disclosure statement;
- Audit reports;
- Government CAs' certificates and certificates issued by the Government CAs.

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

The AGCE 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, AGCE operations team maintains documents making certain disclosures about the Government CAs' practices, procedures and the content of some of its policies, including this CP/CPS. AGCE will at all times make available the current versions of the Government Certification Authority CP/CPS document on its public repository.

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

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

AGCE 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 AGCE activities, and due to their sensitivity, AGCE 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).

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

- The Government CAs publish CRLs including any changes since the publication of the previous CRL, at regular intervals.
- AGCE 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 Government CAs.

AGCE 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 Government CAs and OCSP certificates are published to the AGCE public repository as part of the ceremony completion.

A CRL is issued by the Government CAs every twelve months. In addition, a new CRL will be generated and published following the revocation or issuance of any certificate.

The PKI GB ensures that this CP/CPS is reviewed at least once annually and makes appropriate changes so that the CAs 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 (07) maximum after the PKI GB and the PMA approval.

2.4 Access controls on repositories

Public read-only access is given to the AGCE repository. Security controls are implemented on the repository by AGCE's 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 Government CAs 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 **Government CA** DN is as follows:

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

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

- **CountryName** : DZ
- **stateOrProvinceName** : Algiers

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

The **Government TLS CA** DN is as follows:

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

The **Government TLS CA OCSP** certificates bear the following DN:

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

The **Government CS CA** DN is as follows:

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

The **Government CS CA OCSP** certificates bear the following DN:

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

The **Government SMIME CA** DN is as follows:

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

The **Government SMIME CA OCSP** certificates bear the following DN:

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

The **Government TS CA** DN is as follows:

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

The **Government TS CA OCSP** certificates bear the following DN:

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

The **Corporate CA** DN is as follows:

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

The **OV TLS CA** DN is as follows:

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

The **Code Signing CA** DN is as follows:

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

The **SMIME CA** DN is as follows:

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

The **Trust Services CA** DN is as follows:

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

Government TSP CAs have a DN structured as follows:

- **CountryName** : DZ
- **OrganizationName**: Name of the TSP organisation
- **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

AGCE 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 Government CAs 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

AGCE enforces validation of the proof of possession of the private key as part of the certificate request processing. Proof of possession is provided by submitting CSRs in PKCS#10 format.

3.2.2 Authentication of Organization Identity

Subscribing CAs – AGCE issuing CA

The AGCE PKI GB and RA approves the establishment of the AGCE issuing CAs through a formal internal process involving the top management of AGCE and the PKI GB director.

Subscribing CAs – Government TSP

The identification of the subject in the certificates issued by the Government CAs is validated against the exact meaningful denomination, as agreed with the official representatives of the TSP.

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

- Signature of a registration / certificate request form by the TSP representative;
- AGCE RA using the Algerian Official Journal (Journal Officiel) 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 AGCE RA, as part of the verification process;
- review and validation by the PKI GB of the requesting entity CPS;
- validation of the existence of the requesting entity using the Algerian Official journal;
- site visit by a AGCE 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 Authentication of Individual Identity

The Government CAs does not issue certificates for individuals.

3.2.4 Non-verified Subscriber Information

All subscriber information contained within certificates issued by the Government CAs shall be verified by AGCE RA.

3.2.5 Validation of Authority

Refer to section 3.2.2.

3.2.6 Criteria for Interoperation

No trust relationships (i.e. cross-certification) exist 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-Key

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

3.3.2 Identification and Authentication for Re-Key after revocation

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

3.4 Identification and Authentication for Revocation Requests

Subscribing CAs – AGCE issuing CA

For AGCE issuing CAs certificate revocation, the identification and authentication procedures of revocation requests go through an internal AGCE process involving the AGCE operations team and the AGCE PKI GB. An investigation report is delivered for the approval of the PKI GB. If the certificate revocation is due to a key compromise, the AGCE Disaster Recovery and Business Continuity plan will be executed.

Subscribing CAs – Government TSP

For TSP subscribing CAs certificate revocation, 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 AGCE 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 AGCE 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 Government CAs issue certificates to AGCE issuing CAs and TSPs that are within the Government domain.

The TSP for which a certificate has been issued by the Government CAs has an obligation to inform the AGCE 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.

For AGCE issuing CAs, the AGCE RA authorizes the issuance or the revocation of certificates as part of operational key ceremonies, and after the AGCE PKI GB authorizes the respective operation.

For a government TSP subscribing CAs, the AGCE 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 Government CA shall immediately revoke the concerned TSP certificate.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Subscribing CAs – AGCE issuing CA

The AGCE issuing CAs are established as part of internal AGCE processes. The AGCE RA coordinates with the operations team and engages the AGCE PKI GB for approving the certificate applications for the AGCE issuing CAs.

Subscribing CAs – Government TSP

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

4.1.2 Enrolment Process and Responsibilities

Subscribing CAs – AGCE issuing CA

The AGCE PKI GB authorizes the setup of the AGCE issuing CA. The AGCE RA performs all necessary internal verification involving the operations team. These verifications include the following steps:

- The conclusion of internal ceremony dry runs and a resulting report from the PKI GB audit function;
- The readiness of necessary key ceremony documents related to certifying AGCE issuing CA;
- The confirmation from AGCE PKI operations manager on the readiness of the operations team to operate the AGCE issuing CAs post the go live ceremonies;
- Approval letter from the PKI GB for executing the necessary key ceremonies.

The certificate application processing for the AGCE issuing CA can then be processed and the related key ceremonies planned and executed according to the AGCE key ceremony procedures.

Subscribing CAs – Government TSP

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

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

- The identification of the Government Entity;
- 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 AGCE PKI GB that other pre-requisites related to establishing the TSP are processed by the PKI GB before the AGCE RA can accept the certificate request.

The AGCE 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

Subscribing CAs – AGCE issuing CA

The AGCE issuing CAs are established as part of internal AGCE processes. The AGCE PKI GB authorizes the setup of the AGCE issuing CA. The AGCE RA performs all necessary internal verification involving the operations team. Refer to clause 4.1 for further details on the verification steps.

After all verification steps are performed successfully, the certificate application processing for the AGCE issuing CA can then be processed, and the related key ceremonies planned and executed according to the AGCE key ceremony procedures.

Subscribing CAs – Government TSP

Certificate applications for the Government CA are received as part of an operational cycle agreed between the AGCE 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 AGCE RA including the verification of the information provided in the certificate request form against the approved CPS versions.

The AGCE RA ensures that certificate applications are only processed if the following conditions are met:

- The existence of the applicant is verified using the Algerian Official Journal (Journal Officiel) which is expected to contain detailed information about the entity including its legal name and authorized official representative. The address of the government entity is also verified through an in-person visit from the AGCE RA to the relevant address;
- The applicant representative's identity is verified through an in-person meeting with the AGCE 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 AGCE PKI GB;
- The cycle of mandated audit is successfully executed by the applicant;
- The above verification steps are always executed by the AGCE RA for each certification management operation with the subscribing entities.

4.2.2 Approval or Rejection of Certificate Applications

Subscribing CAs – AGCE issuing CA

The AGCE issuing CAs are established as part of internal AGCE processes. The AGCE PKI GB authorizes the setup of the AGCE issuing CA after validating that all pre-requisites are met including the fulfilment of all compliance verifications.

Subscribing CAs – Government TSP

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 AGCE 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 AGCE 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

Subscribing CAs – AGCE issuing CA

Certificate issuance operations for AGCE issuing CA are executed in accordance with the AGCE operational key ceremonies.

The AGCE RA gathers all required parties at the AGCE primary facility to execute the certificate generation for the AGCE issuing CA. The pre-conditions for executing the ceremony are documented in clause 4.1 and 4.2. As part of the ceremony, the AGCE RA performs final verification before issuing the certificate. 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 per the provisions of this CP/CPS).

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

Following the successful completion of the ceremony and the issuance of the AGCE issuing CA certificate, the AGCE RA inspects the file contents and performs a verification against the expected certificate format. The certificate is then handed over to the operations team for further processing and import into the target AGCE issuing CA systems. All parties that participated in the ceremony sign a ceremony report.

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

Subscribing CA – Government TSP

The certificate issuance for the government TSP CA is executed in accordance with the AGCE operational key ceremonies.

The AGCE RA gathers all required parties at the AGCE 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 AGCE 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;
- 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 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 AGCE key ceremony documentation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

Following issuance of a certificate, the AGCE RA then handovers the issued certificate to the subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribing CAs – AGCE issuing CA

Following the successful completion of the ceremony and the issuance of the AGCE issuing CA certificate, the AGCE RA edits the file contents and performs a verification against the expected certificate format. The certificate is then handed over to the operations team for further processing and import into the target AGCE issuing CA systems.

The certificate is considered as formally accepted if successfully imported to the target AGCE issuing CA systems. The certificate is then published on the target AGCE CA repository.

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

Subscribing CAs – Government TSP

Following the successful completion of the ceremony and the issuance of the TSP certificate, the AGCE 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 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 operations team publish the certificate on the TSP repository. The AGCE 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 Government 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 AGCE 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 Government 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, AGCE 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 AGCE 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 CP/CPS;
- Protecting the CA private keys (and related secrets) from compromise, loss, disclosure, or otherwise unauthorized use of their private keys;
- Notifying the AGCE 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 CP/CPS for complementary details.

4.5.2 Relying party public key and certificate usage

A party relying on a certificate issued by the Government CAs 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 (it's KeyUsage).

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. 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 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

AGCE 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

Subscribing CAs – AGCE issuing CA

The following events may justify the AGCE issuing CA certificate revocation:

- The PKI GB is made aware that the CA operations (including certificate usage) has not complied with the provisions of this CP/CPS, the issuing CA CPS and TSP CP, and applicable CP or CPS, and WebTrust requirements;
- The regular risk assessment conducted by the AGCE PKI GB shows that the CA certificate contents (e.g. key length, cryptographic algorithm, …etc.) presents an unacceptable risk to the overall AGCE PKI domain;
- AGCE did not successfully complete the regular surveillance audit organized by the PMA, and the documented evidence shows that the AGCE misused its issuing CA certificate, or didn't operate continuously in accordance with the provisions of this CP/CPS and the NR-CA CP/CPS, leading the PMA to conclude that the identified issues cause an unacceptable risk to the WebTrust status of the Algeria national PKI;
- The PMA suspects or determines that revocation of an AGCE issuing CA Certificate is indicated.

Considering the criticality of the operation and its impact on the AGCE PKI domain, the AGCE PKI GB invites the PMA to an exceptional meeting.

This meeting is organized no later than twenty-four (24) hours after the circumstances of certificate revocation were identified. The outcome of this meeting is the establishment of the circumstances triggering the AGCE issuing CA certificate revocation request and the related certificate revocation reason(s). The AGCE PKI GB may request additional information/evidence which shall be provided within a maximum of seventy-two (72) hours. At the end of this process, the AGCE issuing CA certificate revocation is approved by the PKI GB and endorsed by the PMA. This decision is documented in a report signed by the PKI GB and the other parties that participated in the decision making.

The certificate revocation ceremony is planned and executed no later than seventy-two (72) hours after the CA certificate revocation is authorized by the AGCE PKI GB. The revocation ceremony is witnessed by members of the PMA. The outcome of the ceremony shall be as follows:

- The AGCE issuing CA certificate is revoked (with the right revocation reason) on the AGCE PKI system;
- A CRL is generated by the Government CA, placed on the target public repository and made immediately available for relying parties;
- The AGCE PKI GB publishes a notice on its repository containing the details of the certificate being revoked and the revocation circumstances;
- The AGCE PKI GB communicates with the PMA so that the AGCE issuing CA service reference is removed by the PMA from the Algeria National Trust List;
- The AGCE RA ensures that all communication, reports and evidence in relation to the certificate revocation operation is recorded and archived for future use as part of audit processes.

Subscribing CA – Government TSP

The revocation request may be triggered by AGCE or by the TSP. The AGCE 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 AGCE RA that the original certificate request was not authorized and does not retroactively grant authorization;
- AGCE 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;
- AGCE obtains evidence that the Certificate was misused;
- AGCE 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;
- AGCE determines that any of the information appearing in the Certificate is inaccurate or misleading;
- CA termination plan was triggered by AGCE or TSP so that Government CA or Subordinate CA ceases operations for any reason and has not made arrangements as per the CA termination plan;
- AGCE's or Subordinate CA's right to issue Certificates under the provisions of the CP/CPS expires or is revoked or terminated, unless AGCE has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by this CP/CPS.

Whenever any of the above circumstances occur, the following process is executed by the AGCE RA:

- When the revocation request is triggered by the TSP, the AGCE 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 AGCE 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 AGCE PKI GB.
- When the AGCE PKI GB triggers the TSP CA revocation after finding evidence of compromise, or suspected compromise of the TSP CA private key, the AGCE 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;
- AGCE at its own discretion (if for instance a compromise is known for this CA key).

Certificate 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

Subscribing CAs – AGCE issuing CA

Refer to section 4.9.1.

Subscribing CA – Government TSP

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 seventy-two (72 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 AGCE 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.
    - A CRL is generated by the Government CA and placed on the target public location within 24 hours maximum from the revocation;
    - AGCE and the subscriber 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 Certification.Problem@agce.dz.

AGCE 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 AGCE 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 Government CAs.

4.9.7 CRL Issuance Frequency

The Government CA update and reissue CRLs (i) once every twelve months and

(ii) within 24 hours after revoking a Subordinate CA Certificate.

The value of the nextUpdate field of CRL issued by the Government CAs is set to twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

Not stipulation.

4.9.9 Online Revocation/Status Checking Availability

AGCE offers an OCSP responder that conforms to RFC 6960 and whose certificate is signed by the Government CAs. 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 Government CAs.

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.

AGCE OCSP responder supports the HTTP GET method.

AGCE updates information provided via its OCSP responder (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

AGCE OCSP responder that receive a request for status of a certificate that has not been issued (unused certificate serial number), 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.

AGCE 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

AGCE only uses OCSP and CRL as methods for publishing certificate revocation information.

4.9.12 Special Requirements related to Key Compromise

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

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 be published on a public repository which is available to relying parties through HTTP protocol queries.

AGCE 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.

AGCE 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 CP/CPS.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The end of subscription for a TSP is triggered by the termination of the TSP certification services and the TSP undergoing a termination plan with AGCE. Refer to section 4.9.1 for further details.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are not escrowed. AGCE does not support key escrow services.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable. AGCE 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 AGCE operations team to perform the functions of key generation, certificate issuance, certificate revocation, audit, and archival.

The AGCE 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 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 AGCE 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

Government CAs

The AGCE PKI GB ensures that appropriate physical controls are implemented on the AGCE (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 AGCE PKI GB audit function on the AGCE PKI operations;
- Regular formal surveillance audits performed by the PMA on the AGCE PKI operations and coordinated with the AGCE PKI GB audit function.

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

5.1.2 Physical Access

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The AGCE PKI GB follows leading practices and applicable safety regulations in Algeria to ensure the 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 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 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 CA online systems are taken regularly to provide enough recovery information when the recovery of the 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 CA operations team. Adequate back-up facilities ensure that backup copies are transferred to the disaster recovery location where they are stored with the same physical, technical and procedurals controls that apply to the primary facility.

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

Subscribing CAs – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The physical and environmental controls listed in the previous clauses related to the Government CAs, shall apply to the AGCE issuing CAs.

Subscribing CAs – Government TSP

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 Government CAs physical and environmental security controls listed above.

5.2 Procedural Controls

Government CAs

The AGCE PKI GB ensures that the appropriate procedural controls are implemented for the 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 AGCE 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:

- Governance function: Operating as the governance function for the AGCE PKI. It groups the necessary functions for this purpose including policy, compliance, and legal. The PKI governance board provides strategic direction for both PKI operations, Information security teams and key management and continuously supervises them.
- PKI operations function: This structure is responsible for operating the trust services implemented by AGCE. It includes the necessary technical functions including PKI roles and IT operations roles, RA authorization. A service delivery function is dedicated to ensure that the trust services are exposed to AGCE customers with the right level of service quality, and a facility management function to manage and operate the facilities (e.g. datacenter, backup site etc.) dedicated for AGCE PKI.
- Information security function: This structure is responsible for the compliance of the information security management to the enterprise security policies. It includes the necessary security functions to maintain and improve the enterprise cyber and information security programs and activities.
- Key management operation: Trusted roles cleared to operate as key custodians and hold key material and secrets necessary for the execution of the CA operational ceremonies.

5.2.2 Number of Persons Required Per Task

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

Key splitting techniques are defined and enforced as part of the CA key management policies and procedures. This ensures that no single individual may gain access to CA private keys.

PKI operators with HSM administrators are involved in CA key operations, such as CA system start-up and CA system shutdown, key backup or key recovery operation.

The AGCE PKI GB ensures that all operational activity performed by 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 AGCE 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;
- AGCE's dedicated staff (system administrators) issue the necessary IT system credentials for CA staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

AGCE 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 – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The procedural controls listed in the previous clauses related to the Government CAs shall apply to the AGCE issuing CAs.

Subscribing CAs – Government TSP

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

5.3 Personnel Controls

Government CAs

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

The CA's personnel security controls include the following:

5.3.1 Qualifications, Experience, and Clearance Requirements

All 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 AGCE PKI GB. While performing any critical operation on the 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 AGCE 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 CA operations. This training is regularly updated and delivered on a yearly basis to CA personnel.

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

For the purpose of maintaining accountability on 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 AGCE 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 AGCE PKI GB documents all training material and make it available to CA personnel. The PKI GB also ensures that key documentation related to CA operations is made available to the personnel. This includes, at a minimum, this CP/CPS document, security policies and the technical documentation relevant to every trusted role.

5.4 Audit Logging Procedures

Government CAs

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

The AGCE 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 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 CA operations team and may be made available during compliance audits.

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

- Government CAs key life cycle management events, including:
  - Key generation, backup, storage, recovery and destruction
  - Cryptographic device life-cycle management events
- Government CAs and Government 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 exits from the CA facility

In addition, the CA operations team maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers
- Power outages

- Physical access of all persons to sensitive parts of the CA sites
- Backup and restore
- Report of disaster recovery tests
- System upgrades
- Security intrusions attempts, and security alarms triggered by the security components (e.g. firewalls, etc.)

The AGCE PKI GB also ensures that the following information, is maintained (either electronically or manually) by the operations team:

- Physical access logs to the CA facility
- CA personnel, security profiles rotations/changes
- All versions of this CPS
- Vulnerability assessment and penetration testing reports
- PKI GB minutes of meetings
- Compliance internal audit reports
- Current and previous versions of infrastructure plans
- Current and previous versions of configuration and operations manuals

Log entries will include at minimum the following elements:

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

5.4.2 Frequency for Processing and Archiving Audit Logs

The AGCE 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 AGCE PKI GB:

- CA application and security audit logs are reviewed on a daily basis, as part of the regular daily operations;
- On a monthly basis, application and system logs are reviewed to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly;
- On a monthly basis, physical access logs are reviewed with an objective to continuously validate the on-going physical access policies;
- On a quarterly basis, the user management logs on the CA systems are reviewed with an objective to continuously validate the on-going logical access policies;
- At least once yearly, the AGCE PKI GB audit and compliance function executes an internal audit of the 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

AGCE ensures that the audit logs are maintained and retained for a period not less than 2 years:

- Government CAs certificate and key lifecycle management event records (as set forth in Section5.4.1(1)) after the later occurrence of:

    1. The destruction of the CA Private Key; or
    2. The revocation or expiration of the CA certificate

- Government CA Subscribing CAs Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the revocation or expiration of the Subscriber Certificate;

- Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

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

5.4.4 Protection of Audit Log

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

- The CA systems generate 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 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 CA operations personnel.

5.4.5 Audit Log Backup Procedures

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

- Backup media are stored locally in the 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 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 CA systems and infrastructure are subject to regular security assessment as follows:

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

The outcome of the regular assessments and identified issues are made available to the PKI operations management, who is responsible to organize and oversee the execution of the remediation by the respective teams.

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

The AGCE 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 a plan is developed and presented to the PKI GB seeking the necessary approvals to proceed with the remediation implementation.

Subscribing CAs – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The audit and logging security controls listed in the previous clauses related to the Government CAs shall apply to the AGCE issuing CAs.

Subscribing CAs – Government TSP

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

5.5 Records Archival

5.5.1 Types of records archived

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

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

5.5.2 Retention period for archive

The AGCE retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for 7 years after any certificate ceases to be valid.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

Only one version of each digital archive is maintained in the primary and disaster recovery facilities of the CA. The 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 CA systems is synchronized with the time source of a GPS clock. Further, the CA operations team enforce a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection system (internal or external)

Only authorized and authenticated staff are allowed to access archived material. The CA operations team use the 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 – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The audit records archival security controls listed in the previous clauses related to the Government CAs shall apply to the AGCE issuing CAs.

Subscribing CAs – Government TSP

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

5.6 Key Changeover

To minimize impact of key compromise, the Government CAs keys are changed with a frequency that ensures the 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

Government CAs

The PKI GB has a Disaster Recovery and Business Continuity Plan that documents the procedures necessary to restore the 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 – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The incident and compromise handling procedures related to the Government CAs listed above shall apply to the AGCE issuing CAs.

Subscribing CAs – Government TSP

The TSP shall implement incident and compromise handling procedures that at minimum, are in line with the Government CAs 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

Government CAs

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

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

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

Subscribing CAs – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The provisions implemented for the Government CAs, to cope with software/resources/data corruption, shall apply to the AGCE issuing CAs.

Subscribing CAs – Government TSP

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

5.7.3 Entity private key compromise procedures

Government CAs

Compromise of the Government CAs 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 AGCE 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 – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The AGCE issuing CA are subject to private key compromise handling procedures similar to the once described above for the Government CAs.

Subscribing CAs – Government TSP

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

5.7.4 Business continuity capabilities after a disaster

Government CAs

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

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

The 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 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 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 – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the Government CAs. The AGCE issuing CA are setup as part of the subject to business continuity capabilities (after disaster) similar to the once described above for the Government CAs.

Subscribing CAs – Government TSP

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

5.8 CA or RA Termination

Government CAs

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

Subscribing CAs – AGCE issuing CA

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

Subscribing CAs – Government TSP

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

6.1.1 Key Pair Generation

Government CAs

The 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 CA personnel only. The detailed key ceremony activities are documented in the CA key ceremony procedure and related ceremony log. The ceremony involves the execution of technical procedures through which the CA personnel setup the CA software and trigger the CA key pair generation through the HSM. The trusted personnel involved in the key generation ceremony select their own secrets and HSM activation data is then generated. All private key material, secrets and activation data is maintained in tamper evident envelopes during the entire lifecycle of the CA private key.

The key ceremony is then completed including the generation of the CA certificate by the NR-CA.

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

Subscribing CAs – AGCE issuing CA

The key ceremony for an AGCE issuing CA key generation 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 personnel only. The detailed key ceremony activities are documented in key ceremony documentation from the AGCE and related ceremony log.

The ceremony involves the execution of technical procedures through which the operations team setups the issuing CA software and triggers the key pair generation of the issuing CA. The Government CA software rejects the processing of certificate request from a Subscribing CA if the requested public key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

The key ceremony is then completed including the generation of the issuing CA certificate by the Government CA. The private key material, secrets and activation data of the AGCE issuing CA is maintained in tamper evident envelopes during the entire lifecycle of the issuing CA private key.

The AGCE issuing CA Key Generation Ceremony is witnessed by the AGCE PKI GB and the PMA audit functions.

Subscribing CAs – Government TSP

The AGCE PKI GB oversees the establishment of the Government 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 AGCE PKI GB audit function. The security measures that are in place for the key generation of the TSP CAs shall be described in their respective CPS.

6.1.2 Private key delivery to subscriber

The CA does not generate private keys for Subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribing CAs – AGCE issuing CA

For the AGCE issuing CAs, the public key certificate is available as part of the certificate application processing. Refer to clauses 4.3 and 4.4 of this CP/CPS document for further details.

Subscribing CAs – Government TSP

The TSP certificate request is processed as part of Government CA ceremonies which result in the generation of the TSP CA certificate that 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 operations team ensures the CA certificate and the Subordinate CA certificates are published on the AGCE public repository.

6.1.5 Key sizes

Government CAs

The minimum size for the 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

Government CAs

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

Government CAs

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

- Certificates for AGCE Issuing CAs;
- Certificates for Government TSPs;
- And certificates for Government 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 CA operations team implements physical and logical safeguards to prevent unauthorized certificate issuance. The 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 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

Government CAs

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

Subscribing CAs Subscribing CAs 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

Government CAs

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

CA personnel are assigned to the trusted roles by the AGCE PKI GB ensuring segregation of duties and enforcing the principles of multi control and split knowledge. Multi-person control of the 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 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 – AGCE issuing CA

The AGCE issuing CA is deployed in the same facility where the Government CAs are deployed. It is operated by the same operations team operating the CA. The AGCE issuing CA are subject to private key shared control.

Subscribing CAs – Government TSP

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

6.2.3 Private key escrow

Government CAs

Private keys of the Government CAs are not escrowed.

Subscribing CAs

Private keys of the subscribing CAs may not be escrowed.

6.2.4 Private key backup

Government CAs

The CA private key is backed up and stored safely in exclusive safes maintained in the most inner security zones of the PKI facilities. Backup operations are executed as part of the CA key generation ceremonies. The 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 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 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 – AGCE issuing CA

The AGCE issuing CAs are deployed in the same facilities where the Government CAs are deployed. Their key generation ceremonies, including the backup of CA private keys, are subject to the same security measures, dual control and split knowledge that apply to the Government CAs private key backup.

Subscribing CAs – Government TSP

The backup and management of TSP CAs private keys shall be subject to the same security measures and controls that apply to the Government CAs private key backup.

6.2.5 Private key archival

AGCE does not archive the Government CAs private keys.

6.2.6 Private key transfer into or from a cryptographic module

Government CAs

The CA uses FIPS 140-2 Level 3 certified/validated HSMs for the primary and disaster recovery facilities. CA private keys and related secret materials 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 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

The CA key pairs shall only be transferred to another hardware cryptographic token of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control.

At no time shall the CA private key be copied to disk or other media during this operation.

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

Government CAs

The 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 CA key remain active only for the duration of the activity requiring the CA activation (e.g. certification, CRL generation). The details of CA private keys activation are documented in the CA key ceremony documentation.

Subscribing CAs – AGCE issuing CA

Private keys for the AGCE Issuing CAs are activated by a minimum of 3 privileged users using the principles of dual control.

Refer to section 6.2.8 of AGCE CPS for Devices and AGCE CPS for Legal and Natural Person.

Subscribing CAs – Government TSP

TSPs activate their own private keys. Private keys for the Government TSP shall be activated by a minimum of three privileged users using the principles of dual control. The activation procedure shall use a PIN entry device attached to the Government TSP HSM.

6.2.9 Method of deactivating private key

Government CAs

The HSMs used for the CA key ceremony are deactivated at the end of the ceremony which prevents any further use of the CA private keys. This activity applies to the principles of dual control and split knowledge, and is always 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 – AGCE issuing CA

The AGCE issuing CAs are controlled by AGCE and operated by the operations team in charge of the Government CAs. Refer to section 6.2.9 of AGCE CPS for Devices and AGCE CPS for Legal and Natural Person.

Subscribing CAs – Government TSP

Refer to section 6.2.9 of TSP-CA CP.

6.2.10 Method of destroying private key

Government CAs

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

The CA keys are destroyed by permanently removing them from any hardware module the keys are stored on.

The 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 – AGCE issuing CA

Refer to section 6.2.10 of AGCE CPS for Devices and AGCE CPS for Legal Natural Person.

Subscribing CAs – Government TSP

Refer to section 6.2.10 of TSP-CA CP.

6.2.11 Cryptographic Module Rating

Government CAs

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

Subscribing CAs

The subscribing CAs cryptographic modules shall be certified/validated to FIPS 140-2 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

See clause 5.5 for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods

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

Government CAs

The Government CAs certificates are valid for seventeen (17) years, with a key usage period for signing Subscriber certificates of eight (8) years. After eight (8) years, the CA certificate will continue to be used for signing CRL but does not issue any new subscriber certificates.

Subscribing CAs

For TSP subscribing CAs the provisions of this CP/CPS suggest TSP CA certificates valid for nine (9) years, with a key usage period of four (4) years.

6.4 Activation Data

6.4.1 Activation data generation and installation

Government CAs

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

6.4.2 Activation data protection

Government CAs

The CA private key and related HSM activation data is generated during the Government CAs private key generation ceremony. The protection mechanisms applied on the 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 Government CAs 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

Government CAs

The operations team is subject to the security controls documented in the CA policy manual. The 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 CA systems and end-point protection;
- Backup and recovery mechanisms for CA operations;
- Hardening of 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 CA operational processes;
- The CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

The AGCE PKI GB organizes regular (at minimum once a year) internal audit to monitor the CA operations against the target security controls. The 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 Government CAs. This applies to the AGCE issuing CA, as well to other government TSP CAs.

6.5.2 Computer Security Rating

The 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

Government CAs

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

All 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 Government CAs.

6.6.2 Security Management Controls

Government CAs

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

The 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 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 Government CAs.

6.6.3 Life-Cycle Security controls

Refer to 6.5.1.

6.7 Network security controls

Government CAs

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

The CA repository and OCSP responder are online systems supporting the 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 CA systems. These controls and technologies limit the services allowed to and from the CA online services.

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

6.8 Time-stamping

Government CAs

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

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

An NTP server is available as part of the CA connected infrastructure. It is used to synchronize the time of the servers that are part of the 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, CRL, and OCSP Profiles

7.1 Certificate Profile

Corporate CA

Field or Extension	Value
Version	
Version	Version 3 value =2
CertificateSerialNumber	
CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature	
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government CA
Subject Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Corporate CA
Validity	
NotBefore	Certificate generation process date/time.
NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo	
AlgorithmIdentifier	RSA
SubjectPublicKey	Public Key Key length: 4096 (RSA)
SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	
AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)
AccessLocation	http://ocsp.pki.agce.dz
AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
AccessLocation	http://ca.pki.agce.dz/repository/cert/government_ca_1.p7b
crlDistributionPoints	
DistributionPoint	http://ca.pki.agce.dz/repository/crl/government_ca.crl
KeyUsage	Critical

	keyCertSign	True
	cRLSign	True
ExtendedKeyUsage		
	id-kp-clientAuth	True
CertificatePolicies		
	PolicyIdentifier	2.16.12.3.2.1.1
	policyQualifiers:policyQualifierId	id-qt 1
	policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
BasicConstraints	Critical	
	CA	True
	pathLenConstraint	0

OV TLS CA

Field or Extension	Value
Version	
Version	Version 3 value =2
SerialNumber	
CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature	
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government TLS CA
Subject Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	OV TLS CA
Validity	
NotBefore	Certificate generation process date/time.
NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo	
AlgorithmIdentifier	RSA

SubjectPublicKey	Public Key Key length: 4096 (RSA)
SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	
AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)
AccessLocation	http://ocsp.pki.agce.dz
AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
AccessLocation	http://ca.pki.agce.dz/repository/cert/government-tls_ca.p7b
crlDistributionPoints	
DistributionPoint	http://ca.pki.agce.dz/repository/crl/government-tls_ca.crl
KeyUsage	Critical
keyCertSign	True
cRLSign	True
ExtendedKeyUsage	
id-kp-clientAuth	True
id-kp-serverAuth	True
CertificatePolicies	
PolicyIdentifier	2.16.12.3.2.1.1
policyQualifiers:policyQualifierId	id-qt 1
policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
BasicConstraints	Critical
CA	True
pathLenConstraint	0

Code Signing CA

Field or Extension	Value
Version	
Version	Version 3 value =2
SerialNumber	
CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature	
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11

Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government CS CA
Subject Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Code Signing CA
Validity	
NotBefore	Certificate generation process date/time.
NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo	
AlgorithmIdentifier	RSA
SubjectPublicKey	Public Key Key length: 4096 (RSA)
SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	
AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)
AccessLocation	http://ocsp.pki.agce.dz
AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
AccessLocation	http://ca.pki.agce.dz/repository/cert/government-tls_ca.p7b
crlDistributionPoints	
DistributionPoint	http://ca.pki.agce.dz/repository/crl/government-cs_ca.crl
KeyUsage	Critical
keyCertSign	True
cRLSign	True
ExtendedKeyUsage	
id-kp-codeSigning	True
CertificatePolicies	
PolicyIdentifier	2.16.12.3.2.1.1
policyQualifiers:policyQualifierId	id-qt 1

policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
PolicyIdentifier	2.23.140.1.4.2
BasicConstraints	Critical
CA	True
pathLenConstraint	0

SMIME CA

Field or Extension	Value
Version	
Version	Version 3 value =2
SerialNumber	
CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature	
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government SMIME CA
Subject Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	SMIME CA
Validity	
NotBefore	Certificate generation process date/time.
NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo	
AlgorithmIdentifier	RSA
SubjectPublicKey	Public Key Key length: 4096 (RSA)
SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	
AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)

	AccessLocation	http://ocsp.pki.agce.dz
	AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
	AccessLocation	http://ca.pki.agce.dz/repository/cert/government-smime_ca.p7b
	crlDistributionPoints	
	DistributionPoint	http://ca.pki.agce.dz/repository/crl/government-smime_ca.crl
	KeyUsage	Critical
	keyCertSign	True
	cRLSign	True
	ExtendedKeyUsage	
	id-kp-emailProtection	True
	CertificatePolicies	
	PolicyIdentifier	2.16.12.3.2.1.1
	policyQualifiers:policyQualifierId	id-qt 1
	policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
	BasicConstraints	Critical
	CA	True
	pathLenConstraint	0

Trust Services CA

Field or Extension	Value
Version	
Version	Version 3 value =2
SerialNumber	
CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature	
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government TS CA
Subject Distinguished Name	
CountryName	DZ

	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	CommonName	Trust Services CA
Validity		
	NotBefore	Certificate generation process date/time.
	NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo		
	AlgorithmIdentifier	RSA
	SubjectPublicKey	Public Key Key length: 4096 (RSA)
SubjectKeyIdentifier		160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier		160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess		
	AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)
	AccessLocation	http://ocsp.pki.agce.dz
	AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
	AccessLocation	http://ca.pki.agce.dz/repository/cert/government-ts_ca.p7b
crlDistributionPoints		
	DistributionPoint	http://ca.pki.agce.dz/repository/crl/governmen-ts_ca.crl
KeyUsage		Critical
	keyCertSign	True
	cRLSign	True
	ExtendedKeyUsage	
	id-kp-timeStamping	True
CertificatePolicies		
	PolicyIdentifier	2.16.12.3.2.1.1
	policyQualifiers:policyQualifierId	id-qt 1
	policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
	PolicyIdentifier	2.23.140.1.4.2
BasicConstraints		Critical
	CA	True
	pathLenConstraint	0

Subscribing CA certificate profile – TSP issuing CA (EKU id-kp-clientAuth)

Field or Extension	Value
Version	
Version	Version 3 value =2
SerialNumber	
CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature	
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government CA
Subject Distinguished Name	
CountryName	DZ
OrganizationName	Allocated as per certificate request
OrganizationUnitName	Allocated as per certificate request
CommonName	Allocated as per certificate request
Validity	
NotBefore	Certificate generation process date/time.
NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo	
AlgorithmIdentifier	RSA
SubjectPublicKey	Public Key Key length: 4096 (RSA)
SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess	
AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)
AccessLocation	http://ocsp.pki.agce.dz
AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
AccessLocation	http://ca.pki.agce.dz/repository/cert/government_ca_1.p7b
crlDistributionPoints	
DistributionPoint	http://ca.pki.agce.dz/repository/crl/government_ca.crl
KeyUsage	Critical
keyCertSign	True

	cRLSign	True
	ExtendedKeyUsage	
	id-kp-clientAuth	True
	CertificatePolicies	
	PolicyIdentifier	2.16.12.3.2.1.1
	policyQualifiers:policyQualifierId	id-qt 1
	policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
	BasicConstraints	Critical
	CA	True
	pathLenConstraint	0

Subscribing CA certificate profile – TSP issuing CA (EKU id-kp-emailProtection)

Field or Extension		Value
Version		
	Version	Version 3 value =2
SerialNumber		
	CertificateSerialNumber	Must be unique, with 64 bits of output from a CSPRNG
Signature		
	Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	CommonName	Government SMIME CA
Subject Distinguished Name		
	CountryName	DZ
	OrganizationName	Allocated as per certificate request
	OrganizationUnitName	Allocated as per certificate request
	CommonName	Allocated as per certificate request
Validity		
	NotBefore	Certificate generation process date/time.
	NotAfter	Certificate generation process date/time + **[108]** Months
SubjectPublicKeyInfo		
	AlgorithmIdentifier	RSA
	SubjectPublicKey	Public Key Key length: 4096 (RSA)

	SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
	AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
AuthorityInfoAccess		
	AccessMethod	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)
	AccessLocation	http://ocsp.pki.agce.dz
	AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
	AccessLocation	http://ca.pki.agce.dz/repository/cert/government-smime_ca.p7b
crlDistributionPoints		
	DistributionPoint	http://ca.pki.agce.dz/repository/crl/government-smime_ca.crl
KeyUsage	Critical	
	keyCertSign	True
	cRLSign	True
ExtendedKeyUsage		
	id-kp-emailProtection	True
CertificatePolicies		
	PolicyIdentifier	2.16.12.3.2.1.1
	policyQualifiers:policyQualifierId	id-qt 1
	policyQualifiers:qualifier:cPSuri	https://ca.pki.agce.dz/repository/cps
BasicConstraints	Critical	
	CA	True
	pathLenConstraint	0

7.1.1 Version number(s)

X.509 v3 is supported and used for all certificates (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.AGCE certificates are signed using sha256WithRSAEncryption OID=1.2.840.113549.1.1.11

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 Government CAs support CRLs compliant with:

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

The Government CA's CRLs are as follows:

Government CA CRL

Field or Extension	Value
Version	
Version	Version 2
Signature	
AlgorithmIdentifier	OID = 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Issuer	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government CA
Validity	
thisUpdate	<creation time>
NextUpdate	<Creation time> + **12 months**
RevokedCertificates	
Certificate	
CertificateSerialNumber	Serial number of the revoked certificates
revocationDate	UTC date when revocation was processed by the CA

crlEntryExtensions	
CRLReason	As per RFC 5280, Identifies the reason for the certificate revocation
Invalidity Date	Date when the certificate is supposed to be invalid
CRL Extensions	
Authority Key Identifier	160-bit SHA-1 hash of subjectPublicKey of the CA public key
CRL Number	Sequential CRL Number
AuthorityInfoAccess	
AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
AccessLocation	http://ca.pki.agce.dz/repository/cert/government_ca_1.p7b

Government TLS CA CRL

Field or Extension	Value
Version	
Version	Version 2
Signature	
AlgorithmIdentifier	OID = 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Issuer	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government TLS CA
Validity	
thisUpdate	<creation time>
NextUpdate	<Creation time> + **12 months**
RevokedCertificates	
Certificate	
CertificateSerialNumber	Serial number of the revoked certificates
revocationDate	UTC date when revocation was processed by the CA
crlEntryExtensions	
CRLReason	As per RFC 5280, Identifies the reason for the certificate revocation
Invalidity Date	Date when the certificate is supposed to be invalid
CRL Extensions	
Authority Key Identifier	160-bit SHA-1 hash of subjectPublicKey of the CA public key
CRL Number	Sequential CRL Number
AuthorityInfoAccess	

	AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
	AccessLocation	http://ca.pki.agce.dz/repository/cert/government-tls_ca.p7b

Government CS CA CRL

Field or Extension		Value
Version		
	Version	Version 2
Signature		
	AlgorithmIdentifier	OID = 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Issuer		
CountryName		DZ
OrganizationName		AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName		Government CS CA
Validity		
	thisUpdate	<creation time>
	NextUpdate	<Creation time> + **12 months**
RevokedCertificates		
Certificate		
	CertificateSerialNumber	Serial number of the revoked certificates
	revocationDate	UTC date when revocation was processed by the CA
	crlEntryExtensions	
	CRLReason	As per RFC 5280, Identifies the reason for the certificate revocation
	Invalidity Date	Date when the certificate is supposed to be invalid
CRL Extensions		
CRL Number		Sequential CRL Number
Authority Key Identifier		160-bit SHA-1 hash of subjectPublicKey of the CA public key
AuthorityInfoAccess		
	AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
	AccessLocation	http://ca.pki.agce.dz/repository/cert/government-cs_ca.p7b

Government SMIME CA CRL

Field or Extension		Value
Version		
	Version	Version 2
Signature		
	AlgorithmIdentifier	OID = 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Issuer		
CountryName		DZ
OrganizationName		AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName		Government SMIME CA
Validity		
	thisUpdate	<creation time>
	NextUpdate	<Creation time> + **12 months**
RevokedCertificates		
Certificate		
	CertificateSerialNumber	Serial number of the revoked certificates
	revocationDate	UTC date when revocation was processed by the CA
	crlEntryExtensions	
	CRLReason	As per RFC 5280, Identifies the reason for the certificate revocation
	Invalidity Date	Date when the certificate is supposed to be invalid
CRL Extensions		
CRL Number		Sequential CRL Number
Authority Key Identifier		160-bit SHA-1 hash of subjectPublicKey of the CA public key
AuthorityInfoAccess		
	AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
	AccessLocation	http://ca.pki.agce.dz/repository/cert/government-smime_ca.p7b

Government TS CA CRL

Field or Extension	Value
Version	
Version	Version 2
Signature	
AlgorithmIdentifier	OID = 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Issuer	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government TS CA
Validity	
thisUpdate	<creation time>
NextUpdate	<Creation time> + **12 months**
RevokedCertificates	
Certificate	
CertificateSerialNumber	Serial number of the revoked certificates
revocationDate	UTC date when revocation was processed by the CA
crlEntryExtensions	
CRLReason	As per RFC 5280, Identifies the reason for the certificate revocation
Invalidity Date	Date when the certificate is supposed to be invalid
CRL Extensions	
Authority Key Identifier	160-bit SHA-1 hash of subjectPublicKey of the CA public key
CRL Number	Sequential CRL Number
AuthorityInfoAccess	
AccessMethod	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)
AccessLocation	http://ca.pki.agce.dz/repository/cert/government TS_ca.p7b

7.2.1 Version number(s)

The Government CAs 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 in section 7.2 above.

7.3 OCSP Profile

The OCSP profile complies with the requirements of RFC 6960.

The Government CAs OCSP response signing certificates profile are as follows:

Government CA OCSP

Field or Extension		Value
Version		Version 3 value=2
CertificateSerialNumber		At least 64 bits of entropy validated on duplicates.
Signature Algorithm		SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	CommonName	Government CA
Validity		
	NotBefore	Certificate generation process date/time.
	NotAfter	Certificate generation process date/time + **[12]** Months
Subject Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	stateOrProvinceName	Algiers
	CommonName	Government CA OCSP
SubjectPublicKeyInfo		
	AlgorithmIdentifier	RSA
	SubjectPublicKey	Public Key Key length: 2048 or 4096 (RSA)
SubjectKeyIdentifier		160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier		160-bit SHA-1 hash of the issuer CA public key
keyUsage		
	digitalSignature	Critical True
extKeyUsage		
	id-kp-OCSPSigning	True
id-pkix-ocsp-nocheck		True
basicConstraints		Critical False : End entity certificate

Government TLS CA OCSP

Field or Extension		Value
Version		Version 3 value=2
CertificateSerialNumber		At least 64 bits of entropy validated on duplicates.
Signature Algorithm		SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	CommonName	Government TLS CA
Validity		
	NotBefore	Certificate generation process date/time.
	NotAfter	Certificate generation process date/time + **[12]** Months
Subject Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	stateOrProvinceName	Algiers
	CommonName	Government TLS CA OCSP
SubjectPublicKeyInfo		
	AlgorithmIdentifier	RSA
	SubjectPublicKey	Public Key Key length: 2048 or 4096 (RSA)
SubjectKeyIdentifier		160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier		160-bit SHA-1 hash of the issuer CA public key
keyUsage		
	digitalSignature	Critical True
extKeyUsage		
	id-kp-OCSPSigning	True
id-pkix-ocsp-nocheck		True
basicConstraints		Critical False : End entity certificate

Government CS CA OCSP

Field or Extension	Value
Version	Version 3 value=2
CertificateSerialNumber	At least 64 bits of entropy validated on duplicates.
Signature Algorithm	SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
CommonName	Government CS CA
Validity	
NotBefore	Certificate generation process date/time.
NotAfter	Certificate generation process date/time + **[12]** Months
Subject Distinguished Name	
CountryName	DZ
OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
stateOrProvinceName	Algiers
CommonName	Government CS CA OCSP
SubjectPublicKeyInfo	
AlgorithmIdentifier	RSA
SubjectPublicKey	Public Key Key length: 2048 or 4096 (RSA)
SubjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier	160-bit SHA-1 hash of the issuer CA public key
keyUsage	
digitalSignature	Critical True
extKeyUsage	
id-kp-OCSPSigning	True
id-pkix-ocsp-nocheck	True
basicConstraints	Critical False : End entity certificate

Government SMIME CA OCSP

Field or Extension		Value
Version		Version 3 value=2
CertificateSerialNumber		At least 64 bits of entropy validated on duplicates.
Signature Algorithm		SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	CommonName	Government SMIME CA
Validity		
	NotBefore	Certificate generation process date/time.
	NotAfter	Certificate generation process date/time + **[12]** Months
Subject Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	stateOrProvinceName	Algiers
	CommonName	Government SMIME CA OCSP
SubjectPublicKeyInfo		
	AlgorithmIdentifier	RSA
	SubjectPublicKey	Public Key Key length: 2048 or 4096 (RSA)
SubjectKeyIdentifier		160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier		160-bit SHA-1 hash of the issuer CA public key
keyUsage		
	digitalSignature	Critical True
extKeyUsage		
	id-kp-OCSPSigning	True
id-pkix-ocsp-nocheck		True
basicConstraints		Critical False : End entity certificate

Government TS CA OCSP

Field or Extension		Value
Version		Version 3 value=2
CertificateSerialNumber		At least 64 bits of entropy validated on duplicates.
Signature Algorithm		SHA256 with RSA Encryption OID = 1.2.840.113549.1.1.11
Issuer Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	CommonName	Government TS CA
Validity		
	NotBefore	Certificate generation process date/time.
	NotAfter	Certificate generation process date/time + **[12]** Months
Subject Distinguished Name		
	CountryName	DZ
	OrganizationName	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE
	stateOrProvinceName	Algiers
	CommonName	Government TS CA OCSP
SubjectPublicKeyInfo		
	AlgorithmIdentifier	RSA
	SubjectPublicKey	Public Key Key length: 2048 or 4096 (RSA)
SubjectKeyIdentifier		160-bit SHA-1 hash of subjectPublicKey
AuthorityKeyIdentifier		160-bit SHA-1 hash of the issuer CA public key
keyUsage		
	digitalSignature	Critical True
extKeyUsage		
	id-kp-OCSPSigning	True
id-pkix-ocsp-nocheck		True
basicConstraints		Critical False : End entity certificate

7.3.1 Version number(s)

The Government CAs 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 AGCE PKI GB ensures that the Government CAs, Issuing CAs and the TSPs operations are subject to regular internal audits. These audits are planned and executed, at a minimum, once 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 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 NR-CA operations as well as to the NR-CA subscribing CAs including the Government 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 AGCE PKI GB audit function is independent of the CA operations team.

External auditors are independent third party WebTrust practitioners.

8.4 Topics covered by assessment

AGCE is audited for compliance to the following standard:

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

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 AGCE 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 reports are published on the AGCE Public 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 at least every year. Refer to sections 8.1 and 8.6 for further details.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Applicable fees, if any, are to be agreed upon by the AGCE and the government TSPs.

9.1.2 Certificate Access Fees

AGCE may not charge for access to issued certificates.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

AGCE may charge for other services depending on business needs and subject to AGCE PKI GB approval.

9.1.5 Refund Policy

No refunds for any charged fees.

9.2 Financial Responsibility

9.2.1 Insurance coverage

The AGCE PKI GB ensures that the Government CAs and AGCE issuing CAs are covered by existing government insurance provisions.

It is the sole responsibility of TSPs to ensure that the CAs issued to them under the Government CAs are covered by existing government insurance provisions.

9.2.2 Other assets

The AGCE PKI GB maintains sufficient financial resources to support the continuous operations of the Government CAs (and AGCE issuing CAs) and ensure the fulfilment of the CA duties as per the provisions of this CP/CPS.

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The AGCE 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 Government CAs;
- Correspondence between the TSP and the AGCE RA during the certificate management processing (including the collected subscribers' data);
- Contractual agreements between the AGCE and its suppliers;
- AGCE 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 AGCE repository.

9.3.3 Responsibility to protect confidential information

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

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

All communications channels with the AGCE shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the CA systems. This shall include:

- The communications between the AGCE 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 AGCE employees, suppliers and contractors handle personal information in strict confidence under the AGCE 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 AGCE ensures that collected personal information is used for the purpose of certificate life cycle management only as consented by the subscribers.

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The AGCE warrants that their 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, AGCE 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.

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

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

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

The CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the CA were the Subordinate CA issuing the Certificates.

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

The AGCE warrants that each TSP signs a subscriber's agreement that lists the subscriber's obligations (except for AGCE issuing CAs that are owned and operated by AGCE). 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 AGCE 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 AGCE requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of AGCE and the Certificate Beneficiaries. Prior to the issuance of a Certificate, the AGCE SHALL obtain, for its express benefit and the Certificate Beneficiaries, either:

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

The AGCE implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request. The Subscriber Agreement or Terms of Use contain 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 AGCE, both in the certificate request and as otherwise requested by AGCE in connection with the issuance of the Certificate(s) to be supplied by the 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 AGCE instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the AGCE 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 Government Certification Authority CP/CPS, or the Baseline Requirements.

9.6.4 Relying parties Representations and Warranties

Relying Parties who rely upon the certificates issued under the Government CAs 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 AGCE 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 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 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 AGCE PKI GB and related to the CA services.

9.8 Limitations of Liability

Limitations on Liability:

- The AGCE 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 AGCE 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 AGCE from and against any such liability and costs and claims arising there from;
- The AGCE 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 AGCE;
- 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 AGCE denies any financial or any other kind of responsibility for damages or impairments resulting from the CA operation.

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

The present CP/CPS is approved by the AGCE PKI GB and the PMA and shall remain in force until amendments are published on AGCE 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 AGCE repository, the newer version becomes effective. The older versions of this document are archived by AGCE 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 AGCE PKI GB reserves the right to change this CP/CPS as and when needed. The PKI GB will incorporate any such change into a new version of this document and, upon PMA approval, publish the new version. The new document will carry a new version number.

9.12.2 Notification Mechanism and Period

Upon publishing on AGCE repository, the newer version of the CP/CPS becomes effective. The older versions of this document are archived on the 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 CA services, shall be first addressed by the AGCE PKI GB legal function. If mediation by the PKI GB legal function is not successful, then the dispute shall be escalated to the PMA then further to be adjudicated by the relevant courts of Algeria if the PMA mediation was not successful.

9.14 Governing Law

The laws of the people's democratic republic of Algeria shall govern the enforceability, construction, interpretation, and validity of this CP/CPS.

9.15 Compliance with applicable law

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

- Law 15-04 fixing "*les règles générales relatives à la signature et à la certification électroniques*" ;
- Décret exécutif N°16-134;
- Décret exécutif N°16-135.
- Law 18-07 on the protection of individuals with regard to the processing of personal data.

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 Government Certification Authority CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of the AGCE.

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 AGCE 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 AGCE 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 AGCE. The AGCE will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS. Any modification to the AGCE practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.