

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
GOVERNMENT ELECTRONIC CERTIFICATION AUTHORITY



AGCE PKI
AGCE CPS for Legal and
Natural Person

Version 2.2

14 September 2023

THE GOVERNMENT TRUST

Document Management

Information

| | |
|---------------------------|---------------------------------------|
| Group of document | AGCE PKI |
| Title | AGCE CPS for Legal and Natural Person |
| Project reference: | Algeria National PKI |
| Annex: | n.a. |

Version control

| Version | Date | Description / Status | Responsible |
|----------------|-------------|---|--------------------|
| V0.1 | 10/10/2019 | Initial version | AGCE |
| V0.2 | 19/12/2019 | Address client comments and produce version ready for final review | AGCE |
| V0.3 | 08/02/2020 | Amended version to accommodate comments received from auditor | AGCE |
| V1.0 | 27/03/2020 | Incorporated final DNs and URLs + correction of typos | AGCE |
| V1.1 | 05/04/2020 | Reviewed the format of CN for legal entities + amended the certificate revocation section with further details | AGCE |
| V1.2 | 05/05/2020 | Amended version with details added to various sections after feedback received from auditor | AGCE |
| V1.3 | 25/10/2020 | Amended versions to accommodate additional feedback from the WebTrust auditor | AGCE |
| V1.4 | 01/10/2021 | Annual review of the CPS. Major changes to accommodate the inclusion of AGCE remote signing service. Also changes to sections 3 and 4 to accommodate the virtual in-person processes while executing identity proofing and related vetting processes. Change in code signing key size to accommodate latest baseline requirements. | AGCE |
| V2.0 | 06/03/2022 | <ul style="list-style-type: none">• 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.• Changes to accommodate the:<ul style="list-style-type: none">○ 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• CPS title changed | AGCE |

| | | | |
|------|------------|--|--|
| V2.1 | 29/05/2023 | <ul style="list-style-type: none"> Updated section 3 and section 4 to add the AGCE RA Officer managing natural person certificates processes SERIALNUMBER field set to mandatory in the natural person certificate profiles A separate HR attestation letter removed for the applicant representative In naming section subjectAltName extension added for email protection certificates Amendments to section 7.1 following the SSL self-assessment report Sanity check | |
| V2.2 | 13/08/2023 | <ul style="list-style-type: none"> Update certificate profiles passed in baseline requirements version 2.0.0 | |

Document Signoff

| Version | Date | Responsible | Validated By | Reviewed and Approved By |
|---------|------------|-------------|---------------------------------|------------------------------|
| V2.2 | 13/08/2023 | AGCE | AGCE (PKI GB) 11 September 2023 | ANCE (PMA) 14 September 2023 |

Table of contents

| | | |
|------------|---|-----------|
| 1 | Introduction | 10 |
| 1.1 | Overview | 11 |
| 1.2 | Document Name and Identification | 13 |
| 1.3 | PKI Participants | 13 |
| 1.3.1 | Certification Authorities | 13 |
| 1.3.2 | Registration Authorities | 13 |
| 1.3.3 | Subscribers | 14 |
| 1.3.4 | Relying Parties | 14 |
| 1.3.5 | Other participants | 14 |
| 1.4 | Certificate Usage | 15 |
| 1.4.1 | Appropriate certificate uses | 15 |
| 1.4.2 | Prohibited certificate uses | 15 |
| 1.5 | Policy Administration | 16 |
| 1.5.1 | Organization Administering the Document | 16 |
| 1.5.2 | Contact person | 16 |
| 1.5.3 | Person Determining CPS Suitability for the Policy | 16 |
| 1.5.4 | CPS approval procedures | 16 |
| 1.6 | Definitions and Acronyms | 16 |
| 1.6.1 | Definitions | 16 |
| 1.6.2 | Acronyms | 20 |
| 1.6.3 | References | 22 |
| 2 | Publication and Repository Responsibilities | 22 |
| 2.1 | Repositories | 22 |
| 2.2 | Publication of Certification Information | 22 |
| 2.3 | Time or Frequency of Publication | 23 |
| 2.4 | Access controls on Repositories | 23 |
| 3 | Identification and Authentication | 24 |
| 3.1 | Naming | 24 |
| 3.1.1 | Types of names | 24 |
| 3.1.2 | Need for names to be meaningful | 25 |
| 3.1.3 | Anonymity or Pseudonymity of Subscribers | 25 |
| 3.1.4 | Rules for Interpreting Various Name Forms | 25 |
| 3.1.5 | Uniqueness of Names | 25 |
| 3.1.6 | Recognition, authentication, and role of Trademarks | 25 |
| 3.2 | Initial Identity Validation | 26 |
| 3.2.1 | Method to Prove Possession of Private Key | 26 |
| 3.2.2 | Authentication of organization identity | 26 |
| 3.2.3 | Authentication of individual identity | 28 |
| 3.2.4 | Non-verified subscriber information | 30 |
| 3.2.5 | Validation of Authority | 30 |
| 3.2.6 | Criteria for Interoperation | 30 |
| 3.3 | Identification and Authentication for Re-key Requests | 30 |
| 3.3.1 | Identification and Authentication for Routine Re-Key | 30 |
| 3.3.2 | Identification and Authentication for Re-Key after revocation | 31 |
| 3.4 | Identification and Authentication for Revocation Request | 31 |
| 4 | Certificate Life-Cycle Operational Requirements | 31 |

| | | |
|------------|--|-----------|
| 4.1 | Certificate Application | 31 |
| 4.1.1 | Who Can Submit a Certificate Application | 31 |
| 4.1.2 | Enrollment Process and Responsibilities | 32 |
| 4.2 | Certificate Application Processing | 33 |
| 4.2.1 | Performing Identification and Authentication Functions | 33 |
| 4.2.2 | Approval or Rejection of Certificate Applications | 34 |
| 4.2.3 | Time to Process Certificate Applications | 35 |
| 4.3 | Certificate Issuance | 35 |
| 4.3.1 | CA Actions during Certificate Issuance | 35 |
| 4.3.2 | Notification to Subscriber by the CA of Issuance of Certificate | 36 |
| 4.4 | Certificate Acceptance | 36 |
| 4.4.1 | Conduct constituting certificate acceptance | 36 |
| 4.4.2 | Publication of the certificate by the CA | 37 |
| 4.4.3 | Notification of certificate issuance by the CA to other entities | 37 |
| 4.5 | Key Pair and Certificate Usage | 37 |
| 4.5.1 | Subscriber private key and certificate usage | 37 |
| 4.5.2 | Relying party public key and certificate usage | 37 |
| 4.6 | Certificate Renewal | 38 |
| 4.6.1 | Circumstance for certificate renewal | 38 |
| 4.6.2 | Who may request renewal | 38 |
| 4.6.3 | Processing certificate renewal requests | 38 |
| 4.6.4 | Notification of new certificate issuance to subscriber | 38 |
| 4.6.5 | Conduct constituting acceptance of a renewal certificate | 38 |
| 4.6.6 | Publication of the renewal certificate by the CA | 38 |
| 4.6.7 | Notification of certificate issuance by the CA to other entities | 38 |
| 4.7 | Certificate Re-key | 38 |
| 4.7.1 | Circumstance for Certificate Re-key | 38 |
| 4.7.2 | Who May Request Certification of a New Public Key | 38 |
| 4.7.3 | Processing Certificate Re-keying Requests | 38 |
| 4.7.4 | Notification of New Certificate Issuance to Subscriber | 39 |
| 4.7.5 | Conduct Constituting Acceptance of a Re-keyed Certificate | 39 |
| 4.7.6 | Publication of the Re-keyed Certificate by the CA | 39 |
| 4.7.7 | Notification of Certificate Issuance by the CA to Other Entities | 39 |
| 4.8 | Certificate Modification | 39 |
| 4.8.1 | Circumstance for Certificate modification | 39 |
| 4.8.2 | Who May Request Certificate modification | 39 |
| 4.8.3 | Processing Certificate Modification Requests | 39 |
| 4.8.4 | Notification of New Certificate Issuance to Subscriber | 39 |
| 4.8.5 | Conduct Constituting Acceptance of a modified Certificate | 39 |
| 4.8.6 | Publication of the modified Certificate by the CA | 39 |
| 4.8.7 | Notification of Certificate Issuance by the CA to Other Entities | 39 |
| 4.9 | Certificate Revocation and Suspension | 39 |
| 4.9.1 | Circumstances for Revocation | 39 |
| 4.9.2 | Who Can Request Revocation | 41 |
| 4.9.3 | Procedure for Revocation Request | 41 |
| 4.9.4 | Revocation Request Grace Period | 43 |
| 4.9.5 | Time within which CA must process the revocation request | 43 |
| 4.9.6 | Revocation Checking Requirement for Relying Parties | 44 |
| 4.9.7 | CRL Issuance Frequency | 44 |
| 4.9.8 | Maximum Latency for CRLs | 44 |
| 4.9.9 | Online Revocation/Status Checking Availability | 44 |
| 4.9.10 | Online Revocation Checking Requirements | 44 |
| 4.9.11 | Other Forms of Revocation Advertisements Available | 45 |
| 4.9.12 | Special Requirements related to Key Compromise | 45 |

| | | |
|-------------|--|-----------|
| 4.9.13 | Circumstances for Suspension | 45 |
| 4.9.14 | Who Can Request Suspension | 45 |
| 4.9.15 | Procedure for Suspension Request..... | 45 |
| 4.9.16 | Limits on Suspension Period..... | 45 |
| 4.10 | Certificate Status Services | 45 |
| 4.10.1 | Operational characteristics | 45 |
| 4.10.2 | Service availability..... | 45 |
| 4.10.3 | Optional features..... | 45 |
| 4.11 | End of Subscription..... | 45 |
| 4.12 | Key Escrow and Recovery | 46 |
| 4.12.1 | Key Escrow and Recovery Policy and Practices..... | 46 |
| 4.12.2 | Session Key Encapsulation and Recovery Policy and Practices..... | 46 |
| 5 | Management, Operational and Physical Controls..... | 46 |
| 5.1 | Physical Security Controls..... | 46 |
| 5.1.1 | Site Location and Construction..... | 47 |
| 5.1.2 | Physical Access..... | 47 |
| 5.1.3 | Power and Air Conditioning | 47 |
| 5.1.4 | Water Exposures | 47 |
| 5.1.5 | Fire Prevention and Protection..... | 47 |
| 5.1.6 | Media Storage | 47 |
| 5.1.7 | Waste Disposal..... | 48 |
| 5.1.8 | Offsite Backup | 48 |
| 5.2 | Procedural Controls | 48 |
| 5.2.1 | Trusted Roles | 48 |
| 5.2.2 | Number of Persons Required Per Task | 49 |
| 5.2.3 | Identification and Authentication for Each Role..... | 49 |
| 5.2.4 | Roles Requiring Separation of Duties..... | 49 |
| 5.3 | Personnel Controls | 49 |
| 5.3.1 | Qualifications, Experience, and Clearance Requirements | 49 |
| 5.3.2 | Background Check Procedures | 50 |
| 5.3.3 | Training Requirements and Procedures | 50 |
| 5.3.4 | Retraining Frequency and Requirements | 50 |
| 5.3.5 | Job rotation frequency and sequence | 51 |
| 5.3.6 | Sanctions for unauthorized actions | 51 |
| 5.3.7 | Independent contractors controls | 51 |
| 5.3.8 | Documentation supplied to personnel..... | 51 |
| 5.4 | Audit Logging Procedures..... | 51 |
| 5.4.1 | Types of Event Recorded..... | 51 |
| 5.4.2 | Frequency for Processing and Archiving Audit Logs..... | 53 |
| 5.4.3 | Retention Period for Audit Log..... | 53 |
| 5.4.4 | Protection of Audit Log | 53 |
| 5.4.5 | Audit Log Backup Procedures | 54 |
| 5.4.6 | Audit Collection System (internal vs. external)..... | 54 |
| 5.4.7 | Notification to Event-causing Subject | 54 |
| 5.4.8 | Vulnerability Assessments..... | 54 |
| 5.5 | Records Archival..... | 54 |
| 5.5.1 | Types of records archived | 54 |
| 5.5.2 | Retention period for archive..... | 54 |
| 5.5.3 | Protection of archive | 55 |
| 5.5.4 | Archive backup procedures..... | 55 |
| 5.5.5 | Requirements for Time-stamping of records | 55 |
| 5.5.6 | Archive Collection System (internal or external) | 55 |
| 5.5.7 | Procedures to obtain and verify archive information..... | 55 |

| | | |
|------------|---|-----------|
| 5.6 | Key Changeover | 55 |
| 5.7 | Compromise and Disaster Recovery | 55 |
| 5.7.1 | Incident and compromise handling procedures..... | 55 |
| 5.7.2 | Computing resources, software, and/or data are corrupted..... | 56 |
| 5.7.3 | Entity private key compromise procedures..... | 56 |
| 5.7.4 | Business continuity capabilities after a disaster..... | 56 |
| 5.8 | CA or RA Termination | 57 |
| 6 | Technical Security Controls | 57 |
| 6.1 | Key Pair Generation and Installation | 57 |
| 6.1.1 | Key Pair Generation..... | 57 |
| 6.1.2 | Private key delivery to subscriber..... | 58 |
| 6.1.3 | Public key delivery to certificate issuer..... | 59 |
| 6.1.4 | CA public key delivery to relying parties..... | 59 |
| 6.1.5 | Algorithm type and key sizes..... | 59 |
| 6.1.6 | Public key parameter generation and quality checking..... | 59 |
| 6.1.7 | Key usage purposes (as per X.509 v3 key usage field)..... | 59 |
| 6.2 | Private Key Protection and Cryptographic Module Engineering Controls | 59 |
| 6.2.3 | Cryptographic module standards and controls..... | 60 |
| 6.2.4 | Private key (n out of m) multi-person control..... | 60 |
| 6.2.5 | Private key escrow..... | 60 |
| 6.2.6 | Private key backup..... | 60 |
| 6.2.7 | Private key archival..... | 60 |
| 6.2.8 | Private key transfer into or from a cryptographic module..... | 60 |
| 6.2.9 | Private key storage on cryptographic module..... | 61 |
| 6.2.10 | Method of activating private key..... | 61 |
| 6.2.11 | Method of deactivating private key..... | 61 |
| 6.2.12 | Method of destroying private key..... | 61 |
| 6.2.13 | Cryptographic Module Rating..... | 62 |
| 6.3 | Other Aspects of Key Pair Management | 62 |
| 6.3.3 | Public key archival..... | 62 |
| 6.3.4 | Certificate operational periods and key pair usage period..... | 62 |
| 6.4 | Activation Data | 62 |
| 6.4.3 | Activation data generation and installation..... | 62 |
| 6.4.4 | Activation data protection..... | 63 |
| 6.4.5 | Other aspects of activation data..... | 63 |
| 6.5 | Computer Security Controls | 63 |
| 6.5.3 | Specific Computer Security Technical Requirements..... | 63 |
| 6.5.4 | Computer Security Rating..... | 64 |
| 6.6 | Life Cycle Technical Controls | 64 |
| 6.6.3 | System Development Controls..... | 64 |
| 6.6.4 | Security Management Controls..... | 64 |
| 6.6.5 | Life-Cycle Security Controls..... | 64 |
| 6.7 | Network security controls | 64 |
| 6.8 | Time-stamping | 65 |
| 6.8.3 | Code Signing Timestamping Services..... | 65 |
| 7 | Certificates, CRL, and OCSP Profiles | 65 |
| 7.1 | Certificate Profile | 65 |
| 7.1.3 | Version number(s)..... | 65 |
| 7.1.4 | Certificate extensions..... | 65 |
| 7.1.5 | Algorithm object identifiers..... | 65 |
| 7.1.6 | Name forms..... | 65 |
| 7.1.7 | Name constraints..... | 65 |

| | | |
|------------|--|------------|
| 7.1.8 | Certificate policy object identifier | 66 |
| 7.1.9 | Usage of Policy Constraints extension..... | 66 |
| 7.1.10 | Policy qualifiers syntax and semantics | 66 |
| 7.1.11 | Processing semantics for the critical Certificate Policies extension | 66 |
| 7.1.12 | Certificates for natural persons | 66 |
| 7.1.13 | Certificates for legal persons..... | 80 |
| 7.2 | CRL Profile..... | 87 |
| 7.2.3 | Issuing CAs CRL..... | 87 |
| 7.2.4 | Version number(s)..... | 92 |
| 7.2.5 | CRL and CRL entry extensions | 92 |
| 7.3 | OCSP Profile..... | 93 |
| 7.3.3 | Issuing CAs OCSP | 93 |
| 7.3.3.3 | SMIME CA OCSP Response Signing Certificate Profile | 97 |
| 7.3.4 | Version number(s)..... | 100 |
| 7.3.5 | OCSP extensions..... | 100 |
| 8. | Compliance Audit and Other Assessments..... | 100 |
| 8.1 | Frequency or circumstances of assessment | 100 |
| 8.2 | Identity / qualifications of assessor | 100 |
| 8.3 | Assessor's relationship to assessed entity | 101 |
| 8.4 | Topics covered by assessment | 101 |
| 8.5 | Actions taken as a result of deficiency | 101 |
| 8.6 | Communication of results..... | 101 |
| 8.7 | Self-audits | 101 |
| 9. | Other Business and Legal Matters | 101 |
| 9.1 | Fees | 101 |
| 9.1.3 | Certificate Issuance or Renewal Fees | 101 |
| 9.1.4 | Certificate Access Fees | 101 |
| 9.1.5 | Revocation or Status Information Access Fees..... | 102 |
| 9.1.6 | Fees for Other Services | 102 |
| 9.1.7 | Refund Policy..... | 102 |
| 9.2 | Financial Responsibility | 102 |
| 9.2.3 | Insurance coverage..... | 102 |
| 9.2.4 | Other assets | 102 |
| 9.2.5 | Insurance or warranty coverage for end-entities | 102 |
| 9.3 | Confidentiality of Business Information | 102 |
| 9.3.3 | Scope of Confidential Information..... | 102 |
| 9.3.4 | Information not within the scope of confidential information | 102 |
| 9.3.5 | Responsibility to protect confidential information..... | 102 |
| 9.4 | Privacy of Personal Information..... | 102 |
| 9.4.3 | Privacy plan..... | 102 |
| 9.4.4 | Information treated as Private | 103 |
| 9.4.5 | Information not Deemed Private | 103 |
| 9.4.6 | Responsibility to protect private information | 103 |
| 9.4.7 | Notice and consent to use private information..... | 103 |
| 9.4.8 | Disclosure Pursuant Judicial or Administrative Process..... | 103 |
| 9.4.9 | Other Information Disclosure Circumstances | 104 |
| 9.5 | Intellectual Property Rights | 104 |
| 9.6 | Representations and Warranties | 104 |
| 9.6.3 | CA Representations and Warranties | 104 |
| 9.6.4 | RA Representations and Warranties | 105 |
| 9.6.5 | Subscriber Representations and Warranties..... | 105 |
| 9.6.6 | Relying parties Representations and Warranties..... | 106 |

| | | |
|-------------|--|------------|
| 9.6.7 | Representations and Warranties of other participants..... | 106 |
| 9.7 | Disclaimers of Warranties | 106 |
| 9.8 | Limitations of Liability..... | 106 |
| 9.9 | Indemnities..... | 107 |
| 9.10 | Term and termination | 107 |
| 9.10.3 | Term..... | 107 |
| 9.10.4 | Termination..... | 107 |
| 9.10.5 | Effect of Termination and Survival..... | 107 |
| 9.11 | Individual notices and communications with participants | 107 |
| 9.12 | Amendments | 107 |
| 9.12.3 | Procedure for Amendment..... | 107 |
| 9.12.4 | Notification Mechanism and Period..... | 107 |
| 9.12.5 | Circumstances Under Which OID Must Be Changed..... | 107 |
| 9.13 | Dispute Resolution Provisions | 108 |
| 9.14 | Governing Law..... | 108 |
| 9.15 | Compliance with applicable law | 108 |
| 9.16 | Miscellaneous provisions | 108 |
| 9.16.3 | Entire Agreement..... | 108 |
| 9.16.4 | Assignment..... | 108 |
| 9.16.5 | Severability | 108 |
| 9.16.6 | Enforcement (Attorney Fees/Waiver of Rights) | 108 |
| 9.16.7 | Force Majeure | 108 |
| 9.17 | Other Provisions..... | 109 |



1 Introduction

The present Certificate Practice Statement (hereinafter, CPS) applies to the certification services of the Issuing CAs established and operated by The Government Authority for Electronic Certification (*Autorité Gouvernementale de Certification Electronique – AGCE*) as part of its PKI services for the Government Domain in Algeria.

In this document, the word “**Issuing CAs**” mean the Issuing CAs of “*Autorité Gouvernementale de Certification Electronique – AGCE*” namely and in the context of this CPS, Corporate CA, SMIME CA and Code Signing CA.

This CPS complies with the Trusted Services Providers (TSP) Certificate Policy that applies to the provision of certification services offered by *Tiers de Confiance (TC) and Prestataires de Service de Certification électronique (PSCE)* issuing certificates to end-entities in Algeria, such as defined and in compliance with the Algerian Law n° 15-04 fixing “*les règles générales relatives à la signature et à la certification électroniques*” [Law 15-04].

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

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

The 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 CPS addresses the technical, procedural and organizational policies and practices of the **Issuing-CAs** about all services available during the lifetime of the below certificates issued by the **Issuing-CAs**:

- **Certificates for natural persons** – certificates issued for citizens and government employees:
 - **Authentication certificate** – used for authentication of end-users to e-services;
 - **Qualified Signing certificate** – used to produce Qualified (high assurance) digital signatures on documents and e-transactions;
 - **Advanced Signing certificate** – used to produce Advanced (moderate assurance) digital signatures on documents and e-transactions;
 - **Email protection certificate** – used to digitally sign email communications.
- **Certificates for legal persons (government entities)** – certificates used for the following purposes:
 - **eSeal certificate** – used to add an eSeal on a document issued/attested by an entity;
 - **Code signing certificate** – used to sign a source code/software developed by an entity.
- **OCSP certificates** – used to sign the Online Certificate Status Protocol (OCSP) responses for certificates issued by the **Issuing-CAs**.

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

Further information about this CPS and the **Issuing-CAs** can be obtained from the AGCE PKI Governance Board (PK GB) using contact information provided in clause 1.5.

1.1 Overview

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

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

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

The Government Authority for Electronic Certification (*Autorité Gouvernementale de Certification Electronique – AGCE*) is established by the Algerian Government to operate the GOV-CA¹ 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 two level CA hierarchy as follows:

- **Government CA:** Intermediate CA certified by the Root CA to sign the following issuing CA:
 - ✓ **Corporate CA:** will issue Digital Signature and Authentication certificates to natural persons (government employees) and legal persons (government entities).
- **Government CS CA:** Intermediate CA certified by the Root CA to sign the following issuing CA:
 - ✓ **Code Signing CA:** will issue code signing certificates to legal persons (government entities).
- **Government SMIME CA:** Intermediate CA certified by the Root CA to sign the following issuing CA:
 - SMIME CA:** will issue email protection (SMIME) certificates to natural persons (government employees).

¹ In this document, the word “GOV-CA” mean the Intermediate CAs of “*Autorité Gouvernementale de Certification Electronique – AGCE*” namely, Government CA, Government CS CA and Government SMIME CA.

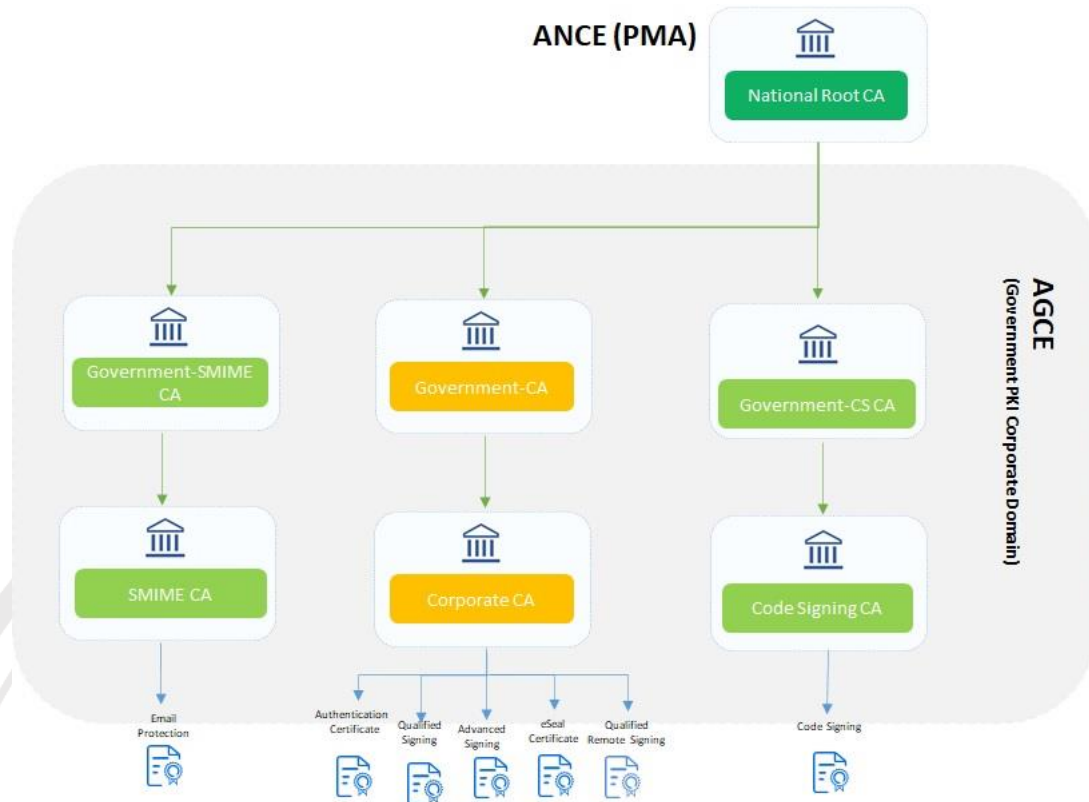


Figure 1: The Government PKI Corporate Domain

In addition to the above issuing CAs, there is a scenario where a Governmental TSPs can establish their own certification services under the GOV-CA². The GOV-CA will certify an issuing CA operated by the TSP. This CA shall be technically constrained where the CA certificate (issued by the GOV-CA) will be populated with a combination of extended key usage and name constraint extensions to limit the scope within which the issuing CA from the TSP may issue end-user certificates;

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

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

² According to TSP CP, a governmental TSPs can establish their own certification services only under Government CA, Government SMIME CA.

1.2 Document Name and Identification

This document is titled “AGCE CPS for Legal and Natural Person” which is identified by the OID 2.16.12.3.2.1.2 and is referenced in related documents as [AGCE CORP-CAs CPS].

1.3 PKI Participants

Several parties make up the participants of these **Issuing-CAs**. The parties mentioned hereunder including these **Issuing-CAs**, the GOV-CAs, subscribers and relying parties. They are referred to collectively as the PKI participants.

1.3.1 Certification Authorities

The AGCE operates the **Issuing-CAs** from dedicated PKI facilities located in Algeria. The **Issuing-CAs** issues certificates in accordance with this CPS and ensures the availability of all services pertaining to the issued certificates, including the issuing, revocation and status verification services.

The 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 PKI operations team. The AGCE PKI GB operating cycle includes interactions with the PMA which is responsible for overseeing the operations of the **Issuing-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 **Issuing-CAs**. It falls under the management and supervision of the PKI GB.

The **Issuing-CAs** are certified by the GOV-CA that is in its turn root-signed by the NR-CA. The PMA seeks 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), accordingly the **Issuing-CAs** shall inherit trust by these programs. This will result in the recognition of the **Issuing-CAs** issued certificates in off-the-shelf applications and web browsers, supporting the technical and trust recognition of the electronic signatures and encrypted emails.

1.3.2 Registration Authorities

AGCE RA

AGCE operates a Registration Authority function for the **Issuing-CAs**, to process certification requests. The RA function falls within the PKI operations structure and responsible for processing certificate management requests for the Algerian government entities.

AGCE RA function is responsible for managing the lifecycle of government entities registered in AGCE’s systems and the processing of certificate management requests of applicants.

The RA function seeks the approval of the PKI GB when applicable See sections 3 and 4 for further details.

Local RAs

AGCE may delegate the RA function to government entities aiming to manage the certificates life cycle for their own user base. In this case, the requesting entity establishes Local Registration Authority (LRA) office in their premises where RA officers belonging to the entity can issue and manage certificates for the entity’s user base. The **Issuing-CAs** only delegates the issuance and management of certificates for natural persons to the LRA.

The AGCE offers an RA delegation model through a Web-based Graphical User Interface (GUI) for Local RA (LRA) officers of third-party government entities in Algeria. An LRA account will be issued for duly authorized officer(s) by the government entity to access the **Issuing-CAs** RA systems. The issued account allows the LRA officer to manage certificate related only to the user base belonging to the government entity.

The entities willing to have a delegated LRA shall sign an agreement with AGCE through which it commits to operate the LRA function in accordance with the TSP CP and this CPS. AGCE LRA agreement enforces the main obligations around end-users (subscribers) identity vetting, key pair generation and certificate lifecycle management.

1.3.3 Subscribers

Subscribers of the **Issuing-CAs** are:

- Employees (and contractors) of government entities;
- Target user base: A Government entity may request certificates to a user base that the entity is authorized to service by law.

The subscribers:

- Are identified in the Subject field of their certificate, issued by the **Issuing-CAs**;
- Control the usage of 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 **Issuing-CAs** using the **Issuing-CAs** Certificate Validity Status Service (e.g. CRL, OCSP), prior to relying on information featured in said certificate.

The **Issuing-CAs** certificates are published on the **AGCE** repository (see clause 2).

1.3.5 Other participants

1.3.5.1 AGCE Remote Signing Service

The AGCE hosts and operates a remote signing service that is responsible for the following operations:

- Generates end-users key pairs inside the HSM connected to the remote signing server. Private Keys are always generated at the request of the end users, cannot be exported from the HSM in an unencrypted form and cannot be used for signing operations without the consent of the legitimate end users.
- Stores securely the generated key-pair in an HSM encrypted form.
- Enables remote generation of digital signature only when this operation is authorized by the end user himself.

The AGCE remote signing service receives the requests for the enrolment of an end-user through the designated AGCE RA or enterprise LRA. The RA completes an identity vetting process with the end user and interacts with the AGCE remote signing server for the remote key pair issuance for the end user, the activation of the remote signing account through a sole control of the end user which results in the issuance of the corresponding end user certificate from the AGCE Corporate CA.

The AGCE remote signing services complies with the two main standards related to remote signing:

- EN 419 241-1: Trustworthy Systems Supporting Server Signing Part 1, General System Security Requirements.
- EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2, Protection Profile for QSCD for Server Signing.

1.4 Certificate Usage

Certain limitations apply to the usage of certificates issued by the **Issuing-CAs** that includes the ones stated hereunder.

1.4.1 Appropriate certificate uses

The certificates issued by **Issuing-CAs** can be used to:

- **Certificates for natural persons:**
 - The following types of certificates are supported by the Corporate CA and may be issued to government employees:
 - **Advanced Signing** – used to produce Advanced (moderate assurance) digital signatures on documents and e-transactions;
 - **Qualified Signing** – used to produce Qualified (high assurance) digital signatures on documents and e-transactions. Issued only to individuals that are identity-vetted through in-person meetings or equivalent with the relevant registration authority. The individual private keys may be use for local or remote signing.
 - **Authentication** – used to authenticate end-users to e-services;
 - The following types of certificates are supported by the SMIME CA and may be issued to government employees:
 - **Email Protection** – used to digitally sign/encrypt email.
- **Certificates for legal persons (government entities):**
 - The following types of certificates are supported by the Corporate CA and may be issued to government entities:
 - **eSeal** – used to add an eSeal on a document issued\attested by a government entity;
 - The following types of certificates are supported by the Code Signing CA and may be issued to government entities:
 - **Code signing** – used to sign a source code/software developed by a government entity.
- **OCSP certificate** – used to sign the Online Certificate Status Protocol (OCSP) responses for certificates issued by the **Issuing-CAs**.

1.4.2 Prohibited certificate uses

Subscribers are authorized to use their certificates for the purposes specified in section 1.4.1 of this document. The use of certificates for any other purposes is strictly prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The AGCE PKI GB has the overall responsibility for producing and publishing this document. 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 CPS;
- Approve the publishing of this CPS and its updates after the completion of a review process with the PMA to continuously ensure this CPS complies with the TSP CP;
- Publishing this CPS and its revisions;
- Conducting regular reviews on the **Issuing-CAs** operations.

1.5.2 Contact person

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

Design 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 PKI GB accepts comments regarding the present 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 private key compromise, certificate misuse, or other types of fraud, inappropriate conduct, or any other matter related to the certificates issued by the **Issuing-CAs** by sending an email to certification.problem@agce.dz.

The AGCE will validate and investigate the revocation 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 CPS. This CPS shall be approved by the PMA as well, since it has to ultimately comply with the provisions of the TSP CP.

1.5.4 CPS approval procedures

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

1.6 Definitions and Acronyms

1.6.1 Definitions

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. For Certificates issued to devices, the

Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

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

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

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

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

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 Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

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

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

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

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

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

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

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

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

Cryptographic Token: A USB cryptographic device certified as conformant with FIPS 140 Level 2 or equivalent.

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

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization. In the context of this CPS, an Enterprise RA is referred to as a Local RA (LRA).

Expiry Date: The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

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.

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

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

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

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

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

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

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

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

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

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

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

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

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

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. In the context of this CPS, the AGCE RA represents the RA function of the Issuing CAs.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate. In the context of this CPS, the Algerian Official Journal (*Journal Officiel*) is the reliable data source for government entities in Algeria.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

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.

Remote Signing Service: For the present CPS, the term Remote Signing Service refers to the service operated by AGCE and that complies with the following remote signing standards:

- ETSI EN 419 241-1: Trustworthy Systems Supporting Server Signing Part 1, General System Security Requirements.
- ETSI EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2, Protection Profile for QSCD for Server Signing.

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.

Request Token: A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; or (ii) a hash of the Subject Public Key Info [X.509]; or (iii) a hash of a PKCS#10 CSR.

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.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

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.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date. **WHOIS:** Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

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 |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| CV | Curriculum Vitae |
| DBA | Doing Business As |
| DN | Distinguished Name |
| DNS | Domain Name System |
| FIPS | Federal Information Processing Standards |
| EID | Electronic Identity Card |
| EIDAS | Electronic IDentification, Authentication and trust Services |
| ETSI | European Telecommunications Standards Institute |

| | |
|---------|---|
| GOV-CA | Government Certification Authority |
| HSM | Hardware Security Module |
| HTTP | Hyper Text Transfer Protocol |
| IANA | Internet Assigned Numbers Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IETF | Internet Engineering Task Force |
| IPSEC | Internet Protocol Security |
| ISO | International Standards Organization |
| IT | Information Technology |
| NR-CA | National Root CA |
| OCSP | Online Certificate Status Protocol |
| LRA | Local Registration Authority |
| LRAO | Local Registration Authority Officer |
| OID | Object Identifier |
| PIN | Personal Information Number |
| PKCS#1 | Public Key Cryptography Standards (PKCS) #1 |
| PKCS#7 | Cryptographic Message Syntax |
| 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 |
| TLD | top-level domain |
| 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 |

1.6.3 References

This CPS endorses the requirements defined in the following:

- TSP CP — Certificate Policy for Trusted Services Providers (TSP) issuing certificates;
- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- AICPA/CPA Canada WebTrust for Certification Authorities Principles And Criteria
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- AICPA/CPA Canada Webtrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates;
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates
- CA/B Forum Network and Certificate System Security Requirements;
- Algerian Law 15-04 on « Digital Signature and Electronic certification » (*Loi n° 15-04 du 01 Février 2015, fixant les règles générales relatives à la signature et à la certification électroniques*)
- Decree 135 (*AGCE décret exécutif N°16-135 fr*);
- EN 419 241-1 — Trustworthy Systems Supporting Server Signing Part 1, General System Security Requirements;
- EN 419 241-2 — Trustworthy Systems Supporting Server Signing Part 2, Protection Profile for QSCD for Server Signing.

2 Publication and Repository Responsibilities

2.1 Repositories

The AGCE publishes information about CA certificates, CRLs for issued certificates, CP/CPS documents and agreements in a public repository that is available 24 × 7 and accessible at <https://ca.pki.agce.dz/repository>.

2.2 Publication of Certification Information

As part of the online repository, the PKI GB maintains documents making certain disclosures about the **Issuing-CAs** practices, procedures and the content of some of its policies, including this CPS. The PKI GB will at all times make available the current versions of the following documentation on its public repository:

- TSP CP;
- CPS of the **Legal and Natural Person**;
- CP/CPS of the Government CA;
- CP/CPS of the Root CA;
- Subscriber agreements;
- Relying party agreements

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

The PKI GB reserves its right to make available and publish information on its practices, as it sees fit.

The **Issuing-CAs** conforms to the current version of the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates. If there is any inconsistency between this document and those requirements, the requirements take precedence over this document.

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

The **Issuing-CAs** publishes digital certificates status information in intervals indicated in this CPS. The provision of **Issuing-CAs** issued electronic certificate validity status information is a 24x7x365 service.

- The **Issuing-CAs** publishes CRLs including any changes since the publication of the previous CRL, at regular intervals. The actual CRL URL to be queried by relying party organizations is referenced in the certificates issued by the **Issuing-CAs**;
- The **Issuing-CAs** 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 **Issuing-CAs**.

The PKI GB 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 **Issuing-CAs** and OCSP certificates are published to the public repository once they are issued.

The **Issuing-CAs** publishes CRLs at regular intervals. The following rules shall apply for the CRLs issued by the **Issuing-CAs**:

- CRLs are refreshed every 24 hours;
- CRLs lifetime shall be set to 26 hours.

The AGCE PKI GB ensures that this CPS is reviewed at least once annually and makes appropriate changes so that the **Issuing-CAs** operations remain fully aligned and in compliance with the requirements listed in the “References” section of this CPS.

Modified versions of the CPS and agreements (Subscriber and Relying party) are published within seven days maximum after the PKI GB and PMA approval.

2.4 Access controls on Repositories

Public read-only access is given to the repository where the AGCE documentation is disseminated (link to the TSP CP, this CPS, certificates and CRLs published to the repository).

Security controls are implemented on the repository by the AGCE operations team to prevent any unauthorized addition, or modification of the data published on the public repository.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The PKI GB ensures that the certification operation for the **Issuing-CAs** is executed in accordance with the provisions of this CPS. This includes the validation of the naming conventions and related parameters used for the certification operation.

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

The PKI GB ensures that proper naming conventions and parameters are enforced throughout the certification cycles with the AGCE RA and through agreement and regular reviews with the LRAs. It also ensures that all information to be included in end-user certificates is verified as part of the certification process.

The DN formats allowed are:

For Certificates issued to Natural persons:

- givenName=<(optional) as on government-issued eID card>;
- surName=<(optional) as on government-issued eID card>;
- SERIALNUMBER = <unique employee identifier or unique national identifier as agreed between the AGCE RA or the LRA and the subscribers>;
- cn= <concatenation of given name and surname as in government-issued eID card separated by a “space” character>;
- ou = <(optional) organizational unit name within a legal entity associated with the natural person>;
- o = <organization name of a legal entity associated with the natural person>;
- l = <(optional if s is present, otherwise mandatory) entity locality name>;
- s = <(optional if l is present, otherwise mandatory) entity province name>;
- subjectAltName = (only for email protection certificates) <email ID that is under the control of the Subscriber >;
- c = DZ.

For Certificates issued to Legal persons:

- cn= <contains the full organization registered name>;
- ou = <(optional) organizational unit name within the legal entity>;
- o = <full registered name of organization to which the certificate is issued>;
- l = <(optional if s is present, otherwise mandatory) name of the locality where the organization is established>;
- s = <(optional if l is present, otherwise mandatory) the province where the organization is established in>;
- c = DZ.

For Corporate CA OCSP certificates:

- cn = Corporate CA OCSP;

- o = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE ;
- s = Algiers;
- c = DZ.

For Code Signing CA OCSP certificates:

- cn = Code Signing CA OCSP;
- o = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE ;
- s = Algiers;
- c = DZ.

For SMIME CA OCSP certificates:

- cn = SMIME CA OCSP;
- o = AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE ;
- s = Algiers;
- c = DZ.

3.1.2 Need for names to be meaningful

The **Issuing-CAs** enforces meaningful names as follows:

For Certificates issued for natural persons: names are meaningful since the CN contains the name of the person.

For Certificates issued for legal persons: names are meaningful since the CN contains a representation of the name of the organization (i.e. commonly used name).

For OCSP certificates: name is meaningful since it indicates the **Issuing-CAs** OCSP name which are “Corporate CA OCSP”, “Code Signing CA OCSP”, “SMIME CA OCSP”

3.1.3 Anonymity or Pseudonymity of Subscribers

This CA does not permit anonymous or pseudonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

The **Issuing-CAs** enforces uniqueness of names as follows:

For Certificates issued for natural persons: uniqueness is enforced through the combination of Surname, Givenname, CN and-the SERIALNUMBER.

For Certificates issued for legal persons: uniqueness is enforced on the CN attribute where a representation of the entity’s legal name is used.

For OCSP certificate: the OCSP name is unique at the **Issuing-CAs** level.

3.1.6 Recognition, authentication, and role of Trademarks

The **Issuing-CAs** requests that subscribers may not request certificates with any content that infringes the intellectual property rights of another entity. However, the **Issuing-CAs** does not verify an Applicant’s right

to use a trademark. The **Issuing-CAs** reserves the right to revoke any certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The AGCE RA systems enforce validation of the proof of possession of the private key as part of the legal person certificate request processing. The proof of possession is submitted to the AGCE RA through CSRs in PKCS#10 format.

3.2.2 Authentication of organization identity

Enrolling organizations and their representatives to the **Issuing-CAs** services is discussed through the following sub-sections.

For certificates issued to the **Issuing-CAs** OCSP, the AGCE RA and an authorized PKI administrator in trusted role oversee the execution of AGCE internal operational ceremonies through which the OCSP certificates are issued. The AGCE GB approves the operational ceremony documentation and validates the embedded certificate templates and naming conventions against the provisions of this CPS. The AGCE GB authorizes then the ceremony and confirms the list of involved AGCE staff.

3.2.2.1 Authentication for organization

This scenario is applicable for government entities that require certificates for legal and natural person. The AGCE RA enrolls the government organization and performs the initial validation of the organization and its representative using the following process:

- a) A representative from the government entity contacts AGCE by sending an email to AGCE team. AGCE RA responds with the necessary information including the application form to be completed by the government entity representative and the AGCE general Terms and Conditions;
- b) The government entity completes the application form with the following minimum information:
 - Government entity's (Organization) legal name;
 - Official address, phone and fax numbers;
 - Name of the official representatives as per the record of the Government entity in the official register of Algeria government entities (referred to as *Journal Officiel* or equivalent);
 - Name of the government entity representative authorized to submit certificate management requests on behalf of the government entity (i.e. applicant representative) for entities applying for legal person certificates, or manages users for entities applying for natural person certificates;
 - Additional information related to the applicant representative (i.e. mobile number and official email address).
- c) The application form is completed by the applicant representative and must be signed by the government entity's official representative. The AGCE subscriber agreement terms and conditions are appended to the signed application form;
- d) The AGCE RA receives the prepared information (application form and other related data) from the applicant representative via an email communication;

Upon receiving the prepared documentation from the government entity's applicant representative, the AGCE RA performs the following minimum mandatory verification steps:

- a) Checking that government entity is not blacklisted using a blacklist maintained by the AGCE RA. If the government entity is in the blacklist, the verification procedure stops, and the government entity's application is declined;
- b) Verifying the legal existence of the government entity in the Algerian Official Journal (*Journal Officiel* or equivalent);
- c) Confirming the government entity address mentioned in the Official Journal or equivalent against the address mentioned in the application form. Also confirming the phone number of the government entity mentioned in the application form by making a random call;
- d) Confirming the applicant representative's email address;
- e) Analyzing all collected/verified information and seeking the AGCE PKI GB approval for enrolling the government entity;
- f) Sending a formal communication to the applicant representative indicating the outcome of the enrolment process. The AGCE RA stores all the communications and exchanges with the government entity.

Furthermore, the AGCE RA may perform a site visit to the government entity with the following objectives:

- In-person identity verification of the applicant representative. Only an official identification document presented by the applicant representative can be used (i.e. government-issued eID card);
- Verification of the government entity address;
- Confirming the authenticity of the government organization application form, the authority of the applicant representative and the authenticity of the attestation letter directly with the government entity official representative.

Upon the approval of the government entity's enrolment, the AGCE RA initiates the internal process through which the government entity and its applicant representative are created on the AGCE Web RA portal in the form of a profile. The information received from the applicant representative is used to populate this profile.

3.2.2.2 DBA/Tradenname

The use of DBA or Tradename in the Subject Identity Information is not supported by the **Issuing-CAs**.

3.2.2.3 Verification of Country

The **Issuing-CAs** issues certificates only to Algerian government entities. The **AGCE RA** verifies that the value of the "country" field of the Subject Identity Information is set to "dz".

3.2.2.4 Authentication for a Local Registration Authority (LRA)

This scenario is applicable for an organization that will require to issue and manage natural person certificates for their user base. The organization and its applicant representative are enrolled by the AGCE RA team in a manner as described in section 3.2.2.1 whereby the government entity official representative signs the AGCE LRA agreement (instead of the subscriber agreement). The applicant representative oversees the operations of the LRA function of the organization and is as such responsible for enrolling the organization LRA officers (LRAO).

Upon the approval of the government entity's enrolment, the AGCE RA initiates the internal process through which the government entity and their LRAOs, are created on the AGCE Web RA portal in the form of a profile. The information received from the organization during the enrolment process is used to populate this profile. The LRAO is enrolled with multi-factor authentication credentials that he can use to execute certificate requests and related certificate management operations.

3.2.3 Authentication of individual identity

This section describes the process followed by the AGCE RA/LRAO for verifying the identity of the natural persons as part of the certificate enrolment processes.

The AGCE RA/LRAO relies on primary and secondary evidences in order to establish the identity of their users. The types of supported evidences are listed below:

- **Primary Evidences:** The accepted primary evidence is the government-issued eID card which is issued with robust identity proofing, issuance and management processes.
- **Secondary Evidences:** Secondary evidences include information extracted from government authoritative sources that are supported by moderate identity proofing, issuance and management processes. Examples of Secondary evidences are: Human Resource (HR) attestation letters, employee certificate or equivalent information establishing the employment relationship between the employee and the government entity, civil servant cards.

The identity proofing process for the different types of individual certificates is listed in the table below:

| Certificate type | Identity verification |
|--|---|
| Advanced signing authentication/Email Protection certificate | <p>An advanced signing certificate is generated in situations where identity proofing through an in-person process cannot be executed with the end-user.</p> <p>The following verification steps are performed:</p> <p>a) The AGCE RA/LRAO obtains the following individual’s identity proofing evidence through the agreed channels:</p> <ul style="list-style-type: none"> • An attestation Letter confirming the affiliation of the individual to the government entity; • A copy of the individual’s government-issued eID card; • An email from HR or a direct line of business manager or applicant representative requesting the AGCE RA/LRAO to enroll the individual into the PKI and issue them certificates of certain types (as per the business need). <p>b) The AGCE RA/LRAO verifies that full name of the individual from the affiliation attestation letter matches the full name from the eID card;</p> <p>c) The AGCE RA/LRAO sends a random verification credential and a series of questions to the individual email. The AGCE RA/LRAO then contacts the individual using his mobile number, verifies full name, date of birth and the verification credential.</p> <p>d) The individual responds to the email received by answering the questions received from The AGCE RA/LRAO.</p> <p>Prior to issuing an email protection certificate, the AGCE RA/LRAO verifies the Domain Name contained in the email address is owned or controlled by the entity in the Organization field by using one of the procedures listed in the AGCE CPS for devices under the section “Validation of Domain Authorization or Control”.</p> |

| | |
|---------------------------------------|---|
| | <p>The identity proofing for the individual completes positively if all the above steps are completed successfully by the AGCE RA/LRAO.</p> |
| <p>Qualified Signing certificates</p> | <p>Identity validation trough an in-person meeting with subscribers</p> <p>The AGCE RA/LRAO validates the individual’s identity through an in-person meeting with the individual and involving the presentation of a government-issued photo eID card (primary evidence) and 2 secondary evidences. The identity verification process is summarized through the followings:</p> <ol style="list-style-type: none"> a) The AGCE RA/LRAO obtains the following individual’s identity proofing evidence through the agreed channels: <ul style="list-style-type: none"> • An attestation Letter in the organization’s letterhead (or an equivalent evidence such as an extract from the Algerian official journal – <i>Journal Officiel</i>) confirming the affiliation of the individual to the government entity and providing details such that full name and date of birth, • A copy of the individual’s government-issued eID card; • An email from HR or a direct line of business manager or applicant representative requesting the AGCE RA/LRAO to enroll the individual into the PKI and issue them certificates of certain types (as per the business need). b) The AGCE RA/LRAO agrees on an in-person meeting with the individual that may happen at the AGCE RA/LRAO office or any other agreed location, c) During the in-person meeting, the individual presents his government-issued eID card to the AGCE RA/LRAO that verifies that full name/date of birth of the individual from the attestation letter matches the full name/date of birth from the eID card. <p>The identity proofing for the individual completes positively if all the above steps are completed successfully by the AGCE RA/LRAO.</p> <p>Identity validation through a live video session with the subscriber</p> <p>When, and only when, it is established that an in-person meeting is not logistically practical for the end-user and/or for the AGCE RA/LRAO, this CPS allows an alternate virtual in-person identity proofing with the AGCE RA/LRAO via a video conference session. This process is summarized through the followings:</p> <ol style="list-style-type: none"> a) The AGCE RA/LRAO obtains the following individual’s identity proofing evidence through the agreed channels: <ul style="list-style-type: none"> • An attestation Letter in the organization’s letterhead confirming the affiliation of the individual to the government entity and providing details such that full name and date of birth; • A copy of the individual’s government-issued eID card; |

| | |
|--|--|
| | <ul style="list-style-type: none"> • An email from HR or a direct line of business manager or applicant representative requesting the AGCE RA/LRAO to enroll the individual into the PKI and issue them certificates of certain types (as per the business need). <p>b) The AGCE RA/LRAO obtains the individual's contact information through the organization's internal processes,</p> <p>c) The AGCE RA/LRAO and the individual agree on a date and time for the live video session,</p> <p>d) During the live video session, the individual presents the front and back sides of his eID card to the AGCE RA/LRAO that verifies that full name/date of birth of the individual from the attestation letter matches the full name/date of birth from the eID card.</p> <p>The identity proofing for the individual completes positively if all the above steps are completed successfully by the AGCE RA/LRAO.</p> |
|--|--|

Upon the initial approval of the individual identity by the AGCE RA/LRAO, the AGCE RA/LRAO initiates a technical procedure through which the individual is enrolled into the Web RA portal where he can execute certificate requests and related certificate management operations.

3.2.4 Non-verified subscriber information

Every subscriber information contained within a certificate issued by the **Issuing-CAs** is verified by the AGCE RA/LRAOs.

3.2.5 Validation of Authority

For certificates issued to Legal persons by AGCE RA: The AGCE RA verifies the authority of the government entity official representative as the signatory of the certificate application form and subscriber agreement. The AGCE RA also verifies the authority of the applicant representative as the person authorized to submit application requests on behalf of the government entity. Refer to sections 3.2.2.1 for further details.

For certificates issued to Natural persons by an organization LRAO: The AGCE RA verifies the authority of the government entity official representative as the signatory of the certificate application form and the LRA agreement. The AGCE RA also verifies the authority of the LRAO as the person authorized to submit application requests on behalf of the government entity. Refer to sections 3.2.2.4 for further details.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The **Issuing-CAs** issues a new certificate to the same subject who has previously been registered in accordance with the same rules and guidance as for the initial request (see sections 3.2.2 and 3.2.3), in addition to the below rules:

- The AGCE RA/LRAO check the existence and validity of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid. All verification/vetting steps are performed by the AGCE RA/LRAO as per section 3.2.2 or 3.2.3 based on the type of certificate;

- If any of the AGCE terms and conditions have changed, these will be communicated by the AGCE RA/LRAO to the subscriber.

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.

3.4 Identification and Authentication for Revocation Request

For Certificates issued for legal persons by the AGCE RA: The identification and authentication procedures of revocation requests involves a formal request from the applicant representative of the entity to which the certificate is issued. 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 subscriber registration);
- Communication with the entity to provide reasonable assurances that the entity's 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.

For Certificates issued for natural persons:

The AGCE RA/LRAO authenticates the revocation request through one of the following methods:

- Receiving a revocation request from a pre-agreed and a concerned department with the government entity (e.g. HR, direct manager of the individual, applicant representative) if the subscriber is terminated or changed role within the entity which would trigger the revocation request. The AGCE RA/LRAO would have the means to confirm with HR or applicant representative the validity of the revocation request;
- Receiving a revocation request from the subscriber through agreed channels with the government entity. This may include a face to face visit to the LRA/AGCE RA, telephone call from the subscriber where the AGCE RA/LRAO asks an identity validation questions (e.g. employee ID, name, date of birth etc.), an email from the subscriber using an email address that can be verified by the AGCE RA/LRAO or through the web RA portal.

For Issuing-CAs OCSP certificates: The present CPS does not specify detailed provisions for revoking any of these AGCE certificates. Such revocation may be triggered by a compromise or suspected compromise of the related private keys which shall be considered by the AGCE as a disaster and treated as such in conformance with the AGCE disaster recovery and business continuity plan. The AGCE RA and an authorized PKI administrator in trusted role oversee the execution of any revocation procedures and shall engage the AGCE GB as required.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

For Certificates issued for legal persons by the AGCE RA: The applicant representative is authorized to submit certificate requests on behalf of the government entity. He is responsible for the authenticity of all data submitted as part of the certificate requests. He ensures the government entity official representative approves the certificate request by signing and stamping the certificate request form and the appended subscriber agreement.

The AGCE RA maintains its own internal blacklist of organizations from which it will not accept certificate requests. The AGCE RA logs in this database previously rejected certificate requests due any to suspected or fraudulent usage and revoked certificate requests from government entities. This internal blacklist database is queried by the AGCE RA whenever it receives any certificate request.

For Certificates issued for natural persons:

Certificate applications may be initiated directly by individuals themselves through the Web RA portal. The AGCE RA/LRAO is authorized to approve and submit the certificate applications. They are responsible for the authenticity of all data submitted as part of the certificate applications. They ensure subscribers agreements are ratified by the individual as part of the certificate request process. The AGCE RA/LRAO maintain a blacklist of individuals affiliated to the government entity for whom certificate requests will not be accepted.

For Issuing-CAs OSCP certificates: The AGCE RA and an authorized PKI administrator in trusted role oversee the execution of AGCE internal operational ceremonies through which OSCP certificates for the **Issuing-CAs** are issued. They engage the AGCE GB for approving the operational ceremony documentation and for validating the embedded certificate templates and naming conventions against the provisions of this CPS. The AGCE GB authorizes the ceremony and confirms the list of involved AGCE staff.

4.1.2 Enrollment Process and Responsibilities

For Certificates issued for legal persons by the AGCE RA:

- The government entity's applicant representative fills and signs the certificate application form shared by AGCE RA. This form is also signed and stamped by the government entity's official representative;
- The relevant technical team from the government entity generates a key pair according to the requirements of this CPS then create a Certificate Signing Request (CSR) using the approved certificate fields in the application form (e.g. DN attributes, key size, key type etc.). This CSR is handed over to the applicant representative;
- The applicant representative authenticates to the web RA portal (using multi-factor authentication) and submits the certificate application including but not limited to the following:
 - Scanned copy of properly filled and signed application form;
 - The information and documents required for identification and authorization;
 - Certificate Signing Request (CSR) file.
- The AGCE RA team reviews and validates the integrity and authenticity of all the submitted documents in addition to vetting the applicant identity as specified in section 3.2.2;
- The AGCE RA team processes the certificate request. Refer to section 4.2.

For Certificates issued on cryptographic tokens for natural persons:

- The individual authenticates to the web RA portal (using multi-factor authentication).
- The individual completes a certificate request form. A technical process is executed that results in the personalization of the token, key pair and CSR generation.
- The individual ratifies the subscriber agreement and submits the certificate request application to the AGCE RA/LRAO.
- The AGCE RA/LRAO is authorized to review and approve the certificate applications. He logs into his Web RA portal and execute the technical steps to verify, approve and submit the certificate request. The AGCE RA/LRAO maintains a blacklist of individuals affiliated to the government entity for whom certificate request will not be accepted.

For remote signing Certificates issued for natural persons:

- The individual authenticates to the web RA portal (using multi-factor authentication) and completes an application form for remote signing key and certificate. As part of this technical process, he ratifies the subscriber agreement.
- The AGCE RA/LRAO is authorized to review and approve the remote signing key and certificate application. He logs into his Web RA portal and execute the technical steps to verify, approve and submit the request for remote signing credentials to AGCE remote signing service. The AGCE RA/LRAO maintains a blacklist of individuals affiliated to the government entity for whom certificate request will not be accepted.

For Issuing-CAs OSCP certificates: The AGCE RA and an authorized PKI administrator in trusted role oversee the execution of AGCE internal operational ceremonies through which any of these certificates can be issued. The AGCE GB approves the operational ceremony documentation and validates the embedded certificate templates and naming conventions against the provisions of this CPS. The AGCE GB authorizes then the ceremony and confirms the list of involved AGCE staff.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Refer to section 3.2.2 or 3.2.3 in addition to the following:

General requirements for all certificate applications:

- a) A unique ID shall be assigned to the request mapped to the certificate application record;
- b) All activities (e-mail communication, phone calls, vetting evidence) are stored by the AGCE RA/LRAO along with the signed certification application form;

For Certificates issued for legal persons by the AGCE RA:

- a) Blacklist check:
 - Using the local blacklist;
 - If the requestor/organization is in the blacklist, the verification procedure is rejected. In case of positive outcome, the vetting procedure continues;
 - Any malicious certificate or revocation request or a request that fails multiple (more than 5) times is added to a dedicated internal blacklist;
 - The internal blacklist is designated per type of certificate and includes the necessary details of the requestor to successfully and unambiguously identify future malicious requests. AGCE maintain its own criteria for identifying high risk certificate requests. Such criteria include 3 consecutive failures for the same certificate requests which will trigger more scrutiny from the AGCE RA in handling future requests from the government entity;
- b) Establish government entity existence: The AGCE RA performs the following verification for each certificate request without relying on previously performed verifications:
 - The government entity requesting a certificate and the organization name to be inserted in the requested certificate must exactly match the legal name of the government entity unless there is an authentic proof linking the entity with the name included in the certificate. The full name or the abbreviated version may be added to the certificate if authorized by law;
 - The government entity existence may be 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;

- In case of negative outcome, the verification procedure stops, the request is rejected, and the request details shall be added to the blacklist. Otherwise, the vetting procedure continues.
- c) Identify government entity authorized representatives: The authorized representatives will be the combination of:
- The applicant representative that signed the certificate request form and submitted the certificate request using his account on the Web RA portal. The AGCE RA identifies the application representative from the certificate request entry on the Web RA portal that will display the name of the certificate request submitter. The name of the certificate request submitter shall be an exact match of the applicant representative created by the AGCE RA during the initial enrolment of the government entity (as described in section 3.2.2.1);
 - The official representative that signed and stamped the certificate request form and the subscriber agreement. He must be formally appointed in this function by the government entity as referenced in the entity's record in the Algerian Official Journal (*Journal Officiel*). The AGCE RA verifies his identity using a process as used during the initial enrolment of the government entity (as described in section 3.2.2.1).

For Code Signing certificates:

The AGCE RA follows the above steps. Moreover, the AGCE RA maintains and implements a documented procedure that identify and require additional verification activity for code signing certificates to ensure that such requests are properly verified and that no one person can single-handedly validate and authorize the issuance of a code signing certificate. The AGCE RA uses the internal blacklist of revoked code signing certificates, due to Code Signatures on Suspect Code and previously rejected certificate requests. The AGCE RA may also query known databases containing information about known or suspected producers, publishers, or distributors of Suspect Code, as identified or indicated by an Anti-Malware Organization.

For Certificates issued for natural persons:

- a) The AGCE RA/LRAO identifies the individual as described in section 3.2.3.
- b) The AGCE RA/LRAO verifies that the individual is not referenced in the blacklist maintained by the AGCE RA/LRAO.
- c) The AGCE RA/LRAO validates the individual's eligibility for the requested certificate according to the government entity's internal processes.
- d) The AGCE RA/LRAO proceeds with the technical procedures related to issuing the requested certificate.

For Issuing-CAs OCSP certificates:

The AGCE RA and an authorized PKI administrator in trusted role oversee the execution of AGCE internal operational ceremonies through which any of these certificates can be issued. The AGCE GB approves the operational ceremony documentation and validates the embedded certificate templates and naming conventions against the provisions of this CPS. The AGCE GB authorizes then the ceremony and confirms the list of involved AGCE staff. The ceremony is executed under the supervision of the AGCE RA that reviews the CSR before its processing by the **Issuing-CAs**.

4.2.2 Approval or Rejection of Certificate Applications

For Certificates issued for legal persons by the AGCE RA: The RA accepts the certificate application and request a digital certificate to the subscriber only when all the below verifications are successful:

- Subject and subscriber identity verification;
- Proof of possession of private key;
- Proof of association with an organization;
- Proof of association between the requesting organization and the subject to which the certificate will be issued;
- Identification and Authorization of the certificate request.

For Certificates issued for natural persons: The AGCE RA/LRAO accepts the certificate application and request a digital certificate to the CA only when all the below verifications are successful:

- Subject (individual) identity is verified;
- Proof of association with the entity (through the attestation letter);
- Eligibility for the requested certificate according to the applicable business rules set by the entity;
- Completion of a certificate application form.

For Issuing-CAs OCSP certificates: A certificate application is approved by the AGCE PKI GB as part of the overall AGCE internal operational ceremony.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

For Certificates issued for legal persons by the AGCE RA: The AGCE RA team to perform the required verification/vetting steps (as per section 4.2.1 of this CPS) and an authorized AGCE PKI administrator in trusted role to issue a direct command for the CA to perform a certificate signing operation.

When the certificate request is submitted to the Corporate CA and/or Code signing CA by the PKI administrator, the CA validates the format and structure of the request then generates the certificate in accordance to the configured certificate template. The certificate is then made available for download by the applicant representative. The CA issues the certificate in “Active” state so that it is ready for use once deployed on the target key-store.

For Certificates issued to cryptographic tokens for natural persons: Certificate issuance by the Corporate CA and/or SMIME CA requires the AGCE RA/LRAO to perform the required verification/vetting steps (as per section 4.2.1 of this CPS) and execute the technical steps and direct commands for submitting the Certificate Signing Request (CSR) to the CA. The CA validates the format and structure of the request then generates the certificate in accordance with the configured certificate template. The certificate then is made available for download from the web RA portal and for import to the user cryptographic token. The CA issues the certificate in “Active” state.

For remote signing Certificates issued for natural persons: Certificate issuance by the Corporate CA requires the AGCE RA/LRAO to perform the required verification/vetting steps (as per section 4.2.1 of this CPS) and to initiate the certificate request to the CA. The AGCE RA/LRAO authenticates to the web RA portal (with multi-factor authentication). He executes technical procedures and direct commands for triggering the generation of the individual’s key-pair on the target key-store (i.e. remote signing HSM) and generating a Certificate Signing Request (CSR).

When the certificate request is submitted to the Corporate CA, the CA validates the format and structure of the request then generates the certificate in accordance with the configured certificate template. The certificate

then is made available for download from the web RA portal. The CA issues the certificate in “Active” state so that it is ready for use.

For Issuing-CAs OCSP certificates: The AGCE RA and an authorized PKI administrator in trusted role oversee the execution of AGCE internal operational ceremonies through which any of these certificates can be issued. The AGCE GB approves the operational ceremony documentation and validates the embedded certificate templates and naming conventions against the provisions of this CPS. The AGCE GB authorizes then the ceremony and confirms the list of involved AGCE staff. The ceremony is executed under the supervision of the AGCE RA. An authorized AGCE PKI administrator in trusted role issues a direct command for the **Issuing-CAs** to perform a certificate signing operation. The issued certificate is reviewed for correctness by the AGCE RA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

For Certificates issued for legal persons by the AGCE RA: The applicant representative is notified by email from the CA that his certificate has been generated. The certificate is made available for download to the subscriber (i.e. applicant representative) on his Web RA portal account.

For Certificates issued for natural persons: The individual (i.e. certificate subscriber) is notified by email from the CA that his certificate has been generated. The certificate is made available for download on his Web RA portal account.

For Issuing-CAs OCSP certificates: The OCSP administrator is notified upon receiving the certificate from AGCE RA team.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

For Certificates issued for legal persons by the AGCE RA: The applicant representative downloads the certificate from the web RA portal. He validates the certificate content against the request made earlier. In case of any discrepancies noted by the applicant representative, he initiates a communication with the AGCE RA through the regular channels (i.e. phone, email) which may lead to initiation of the certificate revocation request by the applicant representative.

In case of no issues in the received certificate, the applicant representative hands the certificate over to the relevant technical team from the government entity that will deploy it on the target key-store. The certificate is deemed accepted by the government entity if no complaints are raised by the applicant representative to the AGCE RA within 10 business days from receiving the certificate.

For Certificates issued for natural persons:

| Certificate type | Conduct constituting certificate acceptance |
|---|--|
| Qualified remote signing certificates for natural persons | <p>The individual downloads the certificate from the web RA portal. He validates the certificate content against the request made earlier. In case of any discrepancies noted by the individual, he initiates a communication with the AGCE RA/LRAO through the regular channels (i.e. phone, email, in-person) which may lead to initiation of the certificate revocation request by the individual or AGCE RA/LRAO.</p> <p>The certificate is deemed accepted by the individual if no complaints are raised by the individual to the AGCE RA/LRAO within 5 business days from receiving the certificate.</p> |

| | |
|--|--|
| <p>Certificates for natural persons issued on cryptographic tokens</p> | <p>In case of any issues with the received certificate and token that may not be usable, the individual (i.e. subscriber) initiates a communication with the AGCE RA/LRAO through the agreed channels (i.e. phone, email, in-person) which may lead to initiation of the certificate revocation request by the AGCE RA/LRAO. The certificate is deemed accepted by the individual if no complaints are raised to the AGCE RA/LRAO within 5 business days from receiving the certificate and token.</p> |
|--|--|

For Issuing-CAs OCSP certificates: The OCSP certificate is deployed on the OCSP key store as part of the AGCE internal operational ceremonies.

4.4.2 Publication of the certificate by the CA

This CA does not publish end-user certificates apart from sharing it with the subscribers.

4.4.3 Notification of certificate issuance by the CA to other entities

No Stipulation.

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

The subscriber's responsibilities include:

- Providing correct and up-to-date information to the **Issuing-CAs** as part of his application;
- Not tampering with a certificate;
- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to the TSP CP and this CPS;
- Protecting the private key (and related secrets) from compromise, loss, disclosure, or otherwise from unauthorized use of their private key;
- Notifying the AGCE RA/LRAO immediately if any details in the certificate become invalid, or as a result of any compromise, loss, disclosure, or otherwise unauthorized use;
- Not using the certificate outside its validity period, or after it has been revoked.

Refer to section 9.6.3 of this CPS for complementary details.

4.5.2 Relying party public key and certificate usage

A party relying on a certificate issued by the **Issuing-CAs** shall:

- Use proper cryptographic tools to validate the certificate signature and validity period;
- Ensure that:
 - the public key is appropriate for the intended use as set forth in the TSP CP and this CPS, and
 - such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage and certificate policies extension fields.

- 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 within the validity period.

4.6 Certificate Renewal

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

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

Certificate re-key is supported by the **Issuing-CAs**. The re-key process (including identity validation, certificate issuance and communication to relevant parties) is similar to the initial certificate application.

4.7.1 Circumstance for Certificate Re-key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation. The re-key operation may invalidate any existing active certificates of the same type for the subscriber based on business rules agreed with the subscriber.

4.7.2 Who May Request Certification of a New Public Key

As per initial certificate issuance.

4.7.3 Processing Certificate Re-keying Requests

As per initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As per initial certificate issuance.

4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate modification

The **Issuing-CAs** 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

The **Issuing-CAs** does not allow certificate modification. Refer to section 4.8.1.

4.8.3 Processing Certificate Modification Requests

The **Issuing-CAs** does not allow certificate modification. Refer to section 4.8.1.

4.8.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance.

4.8.5 Conduct Constituting Acceptance of a modified Certificate

The **Issuing-CAs** does not allow certificate modification. Refer to section 4.8.1.

4.8.6 Publication of the modified Certificate by the CA

As per initial certificate issuance.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate issuance.

4.9 Certificate Revocation and Suspension

Suspension of a certificate is not allowed by **Issuing-CAs**. Only permanent certificate revocation is allowed.

4.9.1 Circumstances for Revocation

For Certificates issued for legal persons by the AGCE RA: For certificates issued to legal persons (i.e. code signing/eSeal certificate), the AGCE RA shall process a revocation request and shall ensure that the Corporate CA, Code signing CA revokes the certificate within 24 hours if one or more of the following occurs:

1. The CA receives a revocation request through the agreed channels from the applicant representative;
2. It was discovered that the original certificate request was not authorized and does not retroactively grant authorization.

3. The CA obtains reasonable evidence that the subscriber's private key, corresponding to the public key certificate, has been compromised;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;

For certificates issued to natural persons:

The subscriber may submit a revocation request through the Web RA portal. Such requests will be processed automatically by the CA.

The AGCE RA/LRAO may process revocation requests related to the government entity's user base within 24 hours if one or more of the following occurs:

1. The AGCE RA/LRAO receives a revocation request through the agreed channels. A typical use case would be an employee that is no longer affiliated to the government and for which an exit process is executed including the revocation of his active certificates;
2. A subscriber submits a revocation request to the AGCE RA/LRAO through the available agreed channels (e.g. phone, email);
3. The AGCE RA/LRAO obtains evidence that a subscriber used the certificate in a manner not in accordance with the procedures of this CPS and with the signed subscriber agreement.

For any certificate issued by the Issuing-CAs: The AGCE RA should ensure a certificate revocation is executed within 24 hours and shall revoke a certificate within 5 days if one or more of the following occurs:

- Obtaining evidence that the certificate no longer complies with the requirements of sections 6.1.5 and 6.1.6;
- Obtaining evidence that the certificate was misused;
- Knowing that a subscriber has violated one or more of its material obligations under the subscriber Agreement;
- Made aware of a material change in the information contained in the Certificate;
- Discovering that the certificate was issued in a manner not in accordance with the procedures of this CPS;
- Knowing that any of the information contained in the certificate is inaccurate
- AGCE's right to issue Certificates under the baseline requirements expires or is revoked or terminated, unless AGCE has planned to continue maintaining the CRL/OCSP Repository
- Revocation is required by this CPS;
- Determination that the certificate was issued to an entity other than the one named as the subject of the certificate;
- AGCE received a lawful order from a law enforcement organization in Algeria to revoke a certificate;
- Discovering that there is a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
- The entity or the subscriber has been declared legally incompetent;
- Knowing that a subscriber has violated one or more of its material obligations under the subscriber Agreement.

The AGCE RA may also trigger and execute the revocation of a subscriber certificate within a commercially reasonable timeframe and not exceeding 7 days under the following circumstances:

- A third party (e.g. law enforcement) provides AGCE with information that leads the CA to believe that a code signing certificate is compromised or is being used to sign suspect code;
- An Application Software vendor requests revocation of a code signing certificate;
- If Microsoft, in its sole discretion, identifies a Code Signing as either containing a deceptive name or as being used to promote malware or unwanted software, Microsoft may contact AGCE and request that it revoke the Certificate. AGCE will either revoke the Certificate within a commercially-reasonable timeframe or request an exception from Microsoft within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. If Microsoft does not grant the exception, AGCE will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days;
- The AGCE at its sole discretion triggering the revocation of the **Issuing-CAs** key which will lead to the execution of the related subscriber revocation procedures.

The **Issuing-CAs** does not issue certificate to any Subordinate CA so the following sub-sections focus only on the revocation provisions that apply to end-entity certificates issued by the **Issuing-CAs**.

4.9.2 Who Can Request Revocation

Revocation can be requested by the following entities:

- Revocations can be directly initiated by AGCE RA in the cases described in section 4.9.1;
- A LRAO shall revoke digital certificates corresponding to the government entity's user base in the cases described in section 4.9.1;
- The subscriber shall be able to request the revocation of his certificate;
- Any relying party or application software supplier possessing evidence of compromise of the subscriber's certificate or its usage to promote malware;
- AGCE at its own discretion (if for instance a compromise is known for the CA key);
- Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify AGCE of a suspected reasonable cause to initiate the certificate revocation process.

Only authorized revocation requests shall be accepted.

4.9.3 Procedure for Revocation Request

The AGCE provides a continuous ability for subscribers and LRAOs to submit certificate requests. This is available through an online system that is accessible 24 x 7 to authenticated subscribers and LRA members. Authenticated and approved revocation requests shall be processed promptly as per the time constraints described in section 4.9.5.

Revocation of certificates is done as follows:

Certificate Revocation by AGCE RA:

1. The AGCE RA authenticates the requester's identity where applicable;
2. The AGCE RA team validates the certificate revocation information;

3. The AGCE RA performs any required investigation within the applicable time constraints (as listed in section 4.9.1 of this CPS). This may include any required communication with the certificate subscriber;
4. The RA team instructs the authorized AGCE PKI administrator in trusted role to execute the certificate revocation. The PKI administrator will issue direct command for the **Issuing-CAs** to perform the certificate revocation;
5. The **Issuing-CAs** revoke the certificate and updates OCSP entries;
6. The AGCE RA notifies via email the applicant representative of the completion of the certificate revocation operation;
7. The AGCE RA updates his internal blacklist with the details of the revoked certificate, circumstances for revocation and based on this information, potentially change the risk profile of the applicant in the internal blacklist. Such information will be queried by the AGCE RA prior to processing future certificate requests for the applicant;
8. The AGCE RA team assigns a unique ID to the revocation request. The AGCE RA records the submitted documents under the assigned ID.

Certificate Revocation handling by AGCE RA following a Certificate problems reporting:

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

The **Issuing-CAs** disclose instructions related to certificate revocation and certificate problem reporting on a dedicated page part of 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 based at least on the following criteria:

- The nature of the alleged problem,
- The number of Certificate Problem Reports received about a particular Certificate or Subscriber,
- The entity making the report (for example, a notification from an Anti-Malware Organization or law enforcement agency carries more weight than an anonymous complaint),
- Relevant legislation.

In case a certificate shall be revoked after a certificate problem reporting, AGCE RA ensures steps 4-8, from the previous section, are executed.

Certificate Revocation by an LRAO:

- The LRAO receives a revocation request from the subscriber or from concerned departments within the government entity (e.g. HR in the case of a terminated employee);
- The LRAO validates the identity of the subscriber as described in section 3.4;
- The LRAO may communicate further with the subscriber and/or internally within the organization in relation to the revocation request in order to establish further the revocation circumstances. The LRAO expects an email from the concerned department (e.g. direct line of business, HR) confirming that the LRAO may proceed with the execution of the certificate revocation;

- The LRAO accesses his account on the web RA portal and issues a direct command to the correspondent CA to revoke the subscriber's certificate;
- The **Issuing-CAs** revokes the certificate and issues a new CRL;
- The LRAO notifies via internal communication the concerned departments (e.g. HR, direct line of business) about the completion of the certificate revocation operation;
- If applicable, the LRAO updates his internal blacklist with the details of the subscriber;
- The LRAO sends an email to the AGCE RA to notify them about the certificate revocation including the circumstances of the revocation;
- The LRAO records the internal communication related to the certificate revocation.

Certificate Revocation by a natural person (subscriber):

The subscriber may submit a revocation request through the Web RA portal. Such requests will be processed automatically by the CA that issues a new CRL.

For Issuing-CAs OCSP certificates:

The AGCE RA and an authorized PKI administrator in trusted role oversee the execution of any revocation procedures and shall engage the AGCE GB as required. The present CPS does not specify detailed provisions for revoking any of these AGCE certificates. Such revocation may be triggered by a compromise or suspected compromise of the related private keys which shall be considered by the AGCE as a disaster and treated as such in conformance with the AGCE disaster recovery and business continuity plan. As part of this plan, the PKI GB executes the communication required towards relying parties.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within which CA must process the revocation request

Certification revocation requests must be processed within 24 hours by the AGCE RA or LRAOs.

For certificate problem reports, the AGCE maintains a 24 x 7 ability to respond internally to certificate problem reports and, where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. The AGCE RA begins investigations within 24 hours from receipt. The AGCE RA initiates communication with the government entity and where appropriate, with Algerian law enforcement authorities. A preliminary communication on the certificate problem is sent to the government entity and to the third party that filed the certificate problem report.

The AGCE RA will perform further investigations and involve the AGCE PKI GB, the government entity team as required, the third party that filed the complaint and other entities as required (e.g. law enforcement) to decide whether revocation or other action is warranted based on at least the following criteria:

- The nature and source of the alleged problem and its potential impact on the PKI community;
- Further discussions with third parties (e.g. law enforcement entities);
- The results of technical assessment performed with the government entity team on their infrastructure;
- Any relevant Algerian legislation.

If the investigations enable the AGCE RA to relate the reported incident to certificate revocation circumstances listed in section 4.9.1, then the certificate shall be revoked within a time frame as set forth in Section 4.9.1.

Based on the revocation circumstances, the AGCE RA may agree with the government entity a plan to issue of a new certificate.

For code signing certificates, the AGCE RA shall always follow the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly Trusted Code Signing Certificates.

4.9.6 Revocation Checking Requirement for Relying Parties

Certificate revocation information is offered to relying parties through CRLs published on a publicly available repository and the **Issuing-CAs** OCSP responder.

Certificates issued by the **Issuing-CAs** (except OCSP certificates) include an HTTP based distribution point of the corresponding CRL and an OCSP responder link from where a relying party could get revocation information. It is the relying party's obligation to retrieve and process the most up-to-date revocation information.

4.9.7 CRL Issuance Frequency

The **Issuing-CAs** publishes CRLs at regular intervals. The following rules shall apply for the CRLs issued by the **Issuing-CAs**:

- CRLs are refreshed every 24 hours;
- CRLs lifetime (i.e. value of the nextUpdate field) is set to 26 hours.

4.9.8 Maximum Latency for CRLs

CRLs are issued timely by the **Issuing-CAs** as per the CRL issuance frequency listed in section 4.9.7 of this CPS.

4.9.9 Online Revocation/Status Checking Availability

Each CA from **Issuing-CAs** offers an OCSP responder that conforms to RFC 6960 and whose certificate is signed by the corresponding CA (i.e SMIME CA, Corporate CA, Code Signing CA) . The OCSP responder avails information immediately to relying party applications based on the CA actions on issued certificates.

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 **Issuing-CAs**.

4.9.10 Online Revocation Checking Requirements

The OCSP responder supports both HTTP GET and HTTP POST methods.

The **Issuing-CAs** updates information provided via its OCSP responder

- (i) immediately when status of an issued certificate is changed.
- (ii) within 24 hours after revoking an **Issuing-CAs** Certificate

OCSP responses from this service have a maximum expiration time of ten days.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused" (i.e. not issued by) the **Issuing-CAs**, then the OCSP responder responds with a "revoked" status as defined by RFC 6960.

The AGCE 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 by relevant teams from AGCE.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements related to Key Compromise

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

Refer to section 4.9.1 for subscriber certificate revocation.

4.9.13 Circumstances for Suspension

Certificate suspension is not supported by the **Issuing-CAs**.

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

Refer to section 4.9.6 of this CPS. In addition, the following provisions are made.

4.10.1 Operational characteristics

The **Issuing-CAs** publishes its CRLs at the public repository accessible to relying parties.

The **Issuing-CAs** OCSP responder exposes an HTTP interface that is also publicly available to relying parties.

Revocation entries on a CRL or OCSP responses are not removed until after the expiry date of the revoked certificates except for code signing certificates which remain in the CRLs or OCSP entries for 10 years after their expiry.

4.10.2 Service availability

The repository including the latest CRL shall be available 24X7 for at least 99% of the time.

The **Issuing-CAs** operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

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

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

Subscription period is linked to the certificate validity period. The subscription ends when the certificate is expired or revoked.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by the **Issuing-CAs**.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Management, Operational and Physical Controls

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

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.

AGCE 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 that AGCE has in place to counter such threats.

Based on the Risk Assessment, AGCE 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 Security Controls

The AGCE PKI GB ensures that appropriate physical controls are implemented on the **Issuing-CAs** (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 regularly as follows:

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

The **Issuing-CAs** 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 **Issuing-CAs** systems.

5.1.2 Physical Access

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

5.1.3 Power and Air Conditioning

The design of the facility hosting the **Issuing-CAs** provides UPS and backup generators with enough capability to support the **Issuing-CAs** operations in power failure circumstances. UPS units and stand-by generators are available for entire facility. A fully redundant air-conditioning system is installed in the areas hosting the **Issuing-CAs** systems. All these systems ensure that the **Issuing-CAs** 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 **Issuing-CAs** facility and systems and to minimize the impact of water exposure. These include installing the **Issuing-CAs** 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 **Issuing-CAs** 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 **Issuing-CAs** 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 **Issuing-CAs** 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. The following procedure applies for removable computer media:

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

5.1.8 Offsite Backup

Full and incremental backups of the **Issuing-CAs** online systems are taken regularly to provide enough recovery information when the recovery of the **Issuing-CAs** 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 **Issuing-CAs** operations team. Adequate back-up facilities ensure that backup copies are transferred to the disaster recovery location where it is stored with the same physical, technical and procedural controls that apply to the primary facility.

The backup and recovery system are tested at least once a year in accordance with the **Issuing-CAs** Disaster Recovery plan.

5.2 Procedural Controls

The AGCE PKI GB ensures that the appropriate procedural controls are implemented for **Issuing-CAs** 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:

- PKI system administration: Trusted roles authorized to install and configure the **Issuing-CAs**, and to perform back-up, recovery and maintenance operations. Also authorized to add other users in the target **Issuing-CAs** systems;
- PKI system operation: Trusted roles authorized to execute the **Issuing-CAs** operational cycle and is involved in critical operations such as subscribers' certification operations and **Issuing-CAs** CRLs generation;
- Key management operation: Trusted roles cleared to operate as key custodians and hold key material and secrets necessary for the execution of **Issuing-CAs** operational ceremonies;
- Security officers:
 - HSM administrator: Authorized to hold HSM activation data and secrets necessary for the HSM operation;

- Security operations: Authorized to collect and view the audit logs generated by the **Issuing-CAs** systems as part of the continuous monitoring of the **Issuing-CAs** systems.
- Audit operation: Trusted role authorized to review the **Issuing-CAs** systems audit logs as part of regular internal compliance audits.

5.2.2 Number of Persons Required Per Task

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

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

The AGCE PKI GB ensures that all operational activity performed by **Issuing-CAs** 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;
- **Issuing-CAs** dedicated staff (system administrators) issue the necessary system credentials for **Issuing-CAs** 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).

5.3 Personnel Controls

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

The **Issuing-CAs** 's personnel security controls include the following:

5.3.1 Qualifications, Experience, and Clearance Requirements

All **CAs** 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 AGCE governance document and other internal AGCE documents. While performing any critical operation on the **Issuing-CAs** 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 and Procedures

The AGCE PKI GB makes available relevant technical personnel to perform their respective CA role. A comprehensive training curriculum is prepared and delivered as part of the establishment of the **Issuing-CAs** operations. This training is regularly updated and delivered on a yearly basis to CA personnel. Training is delivered by a mix of CA experienced staff and third-parties specialized in security and PKI.

The training curriculum is delivered by a mix of AGCE 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 **Issuing-CAs** services. In particular, the training curriculum covers basic and advanced topics necessary for the AGCE RA team 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 operational processes;
- PKI RA processes including vetting and verification procedures;
- 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 or rotation in staff shall 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 contractors controls

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 AGCE ensures that the engaged personnel are subject to the same background check, security control and training as AGCE permanent CA staff.

The AGCE ensures that LRA organizations apply the minimum background and security check on its personnel involved as LRAOs. These verifications are performed during frequent audits executed by AGCE compliance functions. Refer to section 8.1.

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 **Issuing-CAs** operations is made available to the personnel. This includes, at a minimum, this CPS document, security policies and the technical documentation relevant to every trusted role.

5.4 Audit Logging Procedures

The **Issuing-CAs** systems operated by the operations team maintains an audit trail for material events and operations executed on the **Issuing-CAs** 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 **Issuing-CAs** security monitoring team, and are also reviewed as part of the regular internal audits performed by the AGCE PKI GB audit function on **Issuing-CAs** 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 **Issuing-CAs**. 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 AGCE and may be made available during compliance audits.

Following events occurring in relation to the **Issuing-CAs** operations are recorded:

- **Issuing-CAs** key life cycle management events, including:
 - Key generation, backup, storage, recovery, archival and destruction;
 - Cryptographic device life-cycle management events.
- **Issuing-CAs** and **Issuing-CAs** Subscriber 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;
 - User management operations;
 - System platform issues (e.g. crashes), hardware failures.

In addition, the **Issuing-CAs** 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 **Issuing-CAs** 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, not produced by the **Issuing-CAs**, is maintained (either electronically or manually) by the PKI operations team:

- Physical access logs to the **Issuing-CAs** 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 **Issuing-CAs** infrastructure plans;
- Current and previous versions of **Issuing-CAs** 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:

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

5.4.3 Retention Period for Audit Log

The **Issuing-CAs** operations team ensures that the audit logs are maintained and retained for a period not less than 2 years:

- **Issuing-CAs** certificate and key lifecycle management event records (as set forth in Section 5.4.1(1)) after the later occurrence of:
 1. The destruction of the **Issuing-CAs** Private Key; or
 2. The revocation or expiration of the **Issuing-CAs** certificates
- **Issuing-CAs** 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 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 **Issuing-CAs** systems generate cryptographically protected audit logs;
- The security of audits is maintained while these logs transit by the backup system and when these logs are archived;
- The access control policies enforced on the **Issuing-CAs** systems ensure 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 **Issuing-CAs** operations personnel.

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the **Issuing-CAs** audit log:

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

- Quarterly automated vulnerability scan of all public and internal IP addresses of **Issuing-CAs** 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 **Issuing-CAs** systems.

The outcome of the regular assessments and identified issues are made available to the **Issuing-CAs** upper 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 (which coincides with the annual external vulnerability and penetration testing exercise), the **Issuing-CAs** higher PKI operational management will develop and present a security plan to the PKI GB seeking the necessary approvals to proceed with the remediation implementation.

5.5 Records Archival

5.5.1 Types of records archived

The CA retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof. Refer to section 5.5.2 for retention period of archived records.

5.5.2 Retention period for archive

The **Issuing-CAs** retains all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for 7 years after any certificate issuance by the **Issuing-CAs** and based on that documentation ceases to be valid.

5.5.3 Protection of archive

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

Archived logs are protected by a combination of physical, procedural and technical security controls as follows. Archived logs are securely maintained using the access control mechanisms enforced by the **Issuing-CAs** support systems. These policies ensure that only read-access is granted to personnel having access to all archived logs as part of their operational duties.

5.5.4 Archive backup procedures

Versions of digital archives are maintained in the primary and disaster recovery facilities of the **Issuing-CAs**. The 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 the **Issuing-CAs** systems is synchronized with the time source of a GPS clock. Further, the **Issuing-CAs** operations team enforce a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection System (internal or external)

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

5.5.7 Procedures to obtain and verify archive information

Refer to clause 5.5.6.

5.6 Key Changeover

To minimize impact of key compromise, the **Issuing-CAs** keys are changed with a frequency that ensures the **Issuing-CAs** 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 CPS document for key changeover frequency.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

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

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

- The conditions for activating the plan;
- Emergency procedures;
- Fallback procedures;
- Resumption procedures;
- A maintenance schedule for the plan;

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

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

The operations team implements the necessary measures to ensure full recovery of the **Issuing-CAs** 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 **Issuing-CAs** operations and that require the execution of specific recovery procedures. If the **Issuing-CAs** 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.

5.7.3 Entity private key compromise procedures

Compromise of the **Issuing-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.

In the situation of a suspected compromise, 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 a compromise/suspected compromise are identified. Refer to sections 4.9.1 and 4.9.3 for further details.

5.7.4 Business continuity capabilities after a disaster

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

Failover scenarios to the **Issuing-CAs** disaster recovery location are made possible considering the **Issuing-CAs** backup system that enables the continuous replication of critical **Issuing-CAs** 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 **Issuing-CAs** critical services at the disaster recovery location within a maximum of twelve (12) hours RTO.

The business continuity and disaster recovery plan include, 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 **Issuing-CAs** key compromise);
8. Procedures for securing the main facility to the extent possible during the period following a disaster and up to recovery of operations in a secure environment in either the main, or secondary site.

5.8 CA or RA Termination

In the event of a termination of the **Issuing-CAs** services, the CA termination plan is executed and it's cover the following actions:

1. Minimize disruption caused by the termination of an Issuing CA is minimized as much as possible;
2. ensure that archived records are retained;
3. ensure subscribers and relying parties are notified;
4. ensure Certificate status information services are maintained for the applicable period;
5. notify the relevant auditors and government entities (i.e. PMA).

Refer to clauses 4.9 and 5.7 of this CPS for complementary information.

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

6.1.1 Key Pair Generation

CA key pair generation

The **Issuing-CAs** key pair is generated within the memory of an HSM certified evaluated to FIPS 140-2 Level 3.

The key generation ceremony is generated in a physically secured environment as described in section 5.1 of this CPS. The **Issuing-CAs** Generation Ceremony is video recorded and video recording is maintained as evidence for auditing purposes. The key generation ceremony is performed in presence of a quorum of authorized persons in trusted role including PKI GB representatives.

The ceremony is subject to the formal authorization of the PKI GB. The detailed key ceremony activities are documented in key ceremony documentation from the AGCE and related ceremony script. The ceremony involves the execution of technical procedures through which the AGCE PKI operations team setup the issuing

CAs software and trigger the **Issuing-CAs** key pairs generation under the principle of multi-person control and split knowledge. The key ceremony is then completed including the generation of the **Issuing-CAs** certificates by the AGCE GOV-CA. All **Issuing-CAs** private key material, secrets and the activation data of the **Issuing-CAs** are maintained in tamper evident envelopes during the entire lifecycle of the **Issuing-CAs** private keys. The **Issuing-CAs** key generation Ceremony is witnessed by the AGCE compliance officer (i.e. internal auditor).

Subscribers key pair generation

The subscriber keys are generated according to the below requirements:

| Certificate Type | Key generation requirements |
|--|---|
| Natural person certificates | <p>For certificates generated on cryptographic token</p> <p>Subscribers' key pairs within the memory of hardware cryptographic devices conforming to FIPS 140 Level 2 and that prevents exportation. Key pairs shall be generated using key generation algorithm and key sizes as specified under sections 6.1.5 and 6.1.6 of this CPS.</p> <p>For qualified remote signing certificate</p> <p>Subscribers keys are generated in a FIPS 140-2 level 3 hardware security module (HSM) operated by AGCE for its qualified remote electronic signature service meeting the requirements of EU Regulation No 910/2014 (eIDAS Regulation). Key pairs are generated using key generation algorithm and key sizes as specified under sections 6.1.5 and 6.1.6 of this CPS.</p> |
| Legal person certificates (including code signing) | The key pair generation is performed by the subscriber using a hardware cryptographic device conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent. Key generation algorithm and key sizes will be used as specified under sections 6.1.5 and 6.1.6 of this CPS. |
| OCSP certificates | The OCSP key pair is generated inside the memory of a FIPS 140-2 level 3 hardware security module. |

The **Issuing-CAs** rejects a certificate request if the requested public key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

6.1.2 Private key delivery to subscriber

| Key/Certificate type | Delivery procedure |
|--|---|
| Private keys (and certificates) for legal persons | Not applicable. Private keys for legal persons are generated by the subscribers. |
| Natural person keys (and certificates) generated on tokens | Not applicable. Private keys are generated on the cryptographic token and held by the subscriber. |
| Remote signing key (and certificate) | Not applicable. Remote private key held encrypted securely by AGCE remote signing service. |

6.1.3 Public key delivery to certificate issuer

The **Issuing-CAs** accepts CSRs (i.e. commands for certificate generation) only if these originate from the AGCE RA or LRAOs that have been authenticated using their web RA portal.

6.1.4 CA public key delivery to relying parties

The **Issuing-CAs** public key certificates are published on the AGCE public repository.

6.1.5 Algorithm type and key sizes

Issuing-CAs

The Corporate CA, Code Signing CA and SMIME CA uses RSA keys with a size of 4096 bits and SHA-256 algorithm.

Subscribers

The subscriber key pair must be at least 2048 bit RSA and not less than 3072 bit RSA for code signing certificate or at least 256 bit ECDSA.

6.1.6 Public key parameter generation and quality checking

Issuing-CAs

The **Issuing-CAs** private and public keys generation is done with state-of-the-art parameter generation. **Issuing-CAs** HSMs and associated software meet FIPS 186-2 requirements for random generation and primality checks. The operations team references the Baseline Requirements Section 6.1.6 on quality checking.

Subscribers

The LRAO uses reasonable techniques to validate the suitability of public keys presented by Subscribers. Known weak keys are tested for and rejected as described in the CA/B Forum Baseline Requirements section 6.1.6.

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

Issuing-CAs

Private Keys corresponding to the **Issuing-CAs** certificates are not used to sign certificates except in the following cases:

1. Subscriber certificates
2. Certificates for the **Issuing-CAs** OCSP responder

The **Issuing-CAs** certificate shall contain a key usage extension in accordance with RFC 5280 with the following value:

- keyCertSign;
- cRLSign.

Subscribers

Certificates issued to subscribers contain a key usage extension depending on their intended business usage in accordance with RFC 5280. Refer to section 7.1 and 7.3 of this CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The **Issuing-CAs** implements physical and logical safeguards to prevent unauthorized certificate issuance. The **Issuing-CAs** 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.

6.2.3 Cryptographic module standards and controls

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

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

The **Issuing-CAs** private keys are continuously controlled by multiple authorized persons. Trusted roles in relation to **Issuing-CAs** private keys (and related activation data) management are documented in the **Issuing-CAs** 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. 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.

6.2.5 Private key escrow

Private keys of the **Issuing-CAs** are not escrowed. Dedicated backup and restore procedures of the **Issuing-CAs** private key are implemented by the PKI GB.

6.2.6 Private key backup

The **Issuing-CAs** private keys are backed up and held stored safely in exclusive safes maintained in the most inner security zones of the PKI facilities. Backup operations are executed as part of the **Issuing-CAs** key generation ceremonies. The **Issuing-CAs** keys 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 **Issuing-CAs** 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 **Issuing-CAs** 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.

6.2.7 Private key archival

The **Issuing-CAs** does not archive the **Issuing-CAs** private keys.

6.2.8 Private key transfer into or from a cryptographic module

The **Issuing-CAs** uses FIPS 140-2 Level 3 certified/validated HSMs for the primary and disaster recovery facilities. The **Issuing-CAs** private keys and related secret material are backed up as part of the audited key generation ceremonies. Key backup operations are executed through HSM token-to-token operations ensuring encrypted key backups are generated with the enforcement of dual control and split knowledge mechanisms. 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 **Issuing-CAs** private keys has been compromised and potentially communicated to an unauthorized person or organization, then the AGCE 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.

6.2.9 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.

6.2.10 Method of activating private key

Issuing-CAs

Private keys for the **Issuing-CAs** are activated by a minimum of 3 privileged users using the principles of dual control and split knowledge. The activation procedure uses a PIN entry device connected to the **Issuing-CAs** HSM.

Subscribers

Natural person private key stored on cryptographic tokens

Subscribers plug in the PKI hardware token to the appropriate reader or slot and when asked they provide the PIN associated with the PKI hardware token to activate their private key.

Remote signing private key for a natural person issued through an LRAO

To activate the subscriber's remote signing private key, the AGCE remote signing service implements a secure protocol that complies with EN 419 241-2 Level of Assurance 2. This protocol requires the involvement of the subscriber to activate his remote signing private key. The subscriber key is activated for every signature transaction.

6.2.11 Method of deactivating private key

Issuing-CAs

Private keys for the **Issuing-CAs** are deactivated in situations such as:

- There is a power failure within the CA room in which case the key partitions are deactivated;
- The CA HSM is operated outside the range of supported temperatures in which case the key partitions are deactivated; or
- The HSM detects a security breach and deletes all key material within its internal memory.

Subscribers

Natural person private key stored on cryptographic tokens

The subscribers simply unplug their PKI hardware token from the appropriate reader or slot to deactivate their private key.

Remote signing private key for a natural person

The subscriber's remote signing key is automatically deactivated after it has been used to sign a transaction.

6.2.12 Method of destroying private key

Issuing-CAs

At the end of their lifetime the private keys are destroyed by at least 3 trusted staff members at the presence of at least one representative of the PKI GB, in order to ensure that these private keys cannot ever be retrieved and used again.

The **Issuing-CAs** keys are destroyed by removing permanently from any hardware modules the keys are stored on.

The decision for private key destruction outside the context of the end of its lifetime needs to be authorized in writing by multiple members of the PKI GB. This decision includes the assignment of the personnel.

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.

Subscribers

Natural person private key stored on cryptographic tokens

The subscriber can delete their keys and certificates from the PKI hardware token using the appropriate vendor's provided software. Alternatively, the subscriber can re-initialize their PKI hardware token to destroy all the contents held in their PKI hardware token.

Remote signing private key for a natural person

The remote signing private key of a subscriber is automatically deleted by the AGCE remote signing service after the revocation or expiry of the corresponding remote signing certificate.

6.2.13 Cryptographic Module Rating

The **Issuing-CAs** uses HSM certified to FIPS 140-2 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.3 Public key archival

See clause 5.5 for archival conditions.

6.3.4 Certificate operational periods and key pair usage period

The **Issuing-CAs** certificate is valid for nine (9) years, with a key usage period of three (4) years.

The **Issuing-CAs** certificate policies ensure that subscriber certificates have a validity period not greater than the maximum lifetime of Subscriber certificate after the latest Subscriber certificate issuance as defined in section 7.1.

6.4 Activation Data

6.4.3 Activation data generation and installation

Issuing-CAs

The **Issuing-CAs** private keys and HSM activation data is generated during the **Issuing-CAs** private key generation ceremony. It is used to activate the CA private key inside the target HSMs. In preparation of the key generation ceremony of the **Issuing-CAs**, AGCE staff in trusted roles are instructed to use strong passwords and PINs. A password policy, that meet the requirements specified by the CAB Forums Network Security Requirements, is distributed to the trusted roles as part of the key ceremony documentation.

Subscribers

Natural person private key stored on cryptographic tokens

Subscriber's private key in the PKI hardware token is protected via a secure PIN that is only known the subscriber.

Remote signing private key for a natural person

Subscriber's remote signing key is protected by the AGCE operated remote signing service. To activate the subscriber's remote signing key, a secure authorization protocol is used. This involves the generation of activation data and the signature of this activation data by the subscriber using an authorization key that is held

in the secure element/secure enclave of the subscriber's registered mobile device. The AGCE remote signing service verifies the signature of the activation data and activates the subscriber's private key.

6.4.4 Activation data protection

Issuing-CAs

The **Issuing-CAs** activation data consists of PINs, passwords and accounts that are used to activate the HSMs hosting the CA keys and the CA keys. The security controls that apply to the CA private key protection will apply to the protection to the related activation data. A combination of physical security, technical and procedural controls ensure that the CA private keys and activation data is protected at all times through its confidentiality, integrity and availability. Refer to section 6.2 of this CPS for further details.

Subscribers

Subscribers shall protect the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure and use of these private keys. Such obligation is presented to the subscribers as part of the Subscriber Agreement.

6.4.5 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

AGCE performs all **Issuing-CAs** and RA functions using trustworthy systems that meet its own policy requirements, the TSP CP and the present CPS requirements.

6.5.3 Specific Computer Security Technical Requirements

The **Issuing-CAs** are operated according to the following security controls:

- Physical access control to the **Issuing-CAs** servers is enforced;
- Separation of duties and dual controls for CA sensitive operations;
- Identification and authentication of PKI roles and their associated identities;
- Archival of CAs history and audit data;
- Audit of security-related events;
- Automatic and regular validation of the CA systems' integrity;
- Recovery mechanisms for keys and CA systems;
- Hardening CA servers' operating system according to best practices and PKI vendor requirements;
- Continuous monitoring of **Issuing-CAs** systems and end-point protection;
- In-depth network security architecture including perimeter and internal firewalls, web application firewalls, including intrusion detection systems;
- Proactive patch management as part of the **Issuing-CAs** operational processes.

The **Issuing-CAs** and RA 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 **Issuing-CAs** operations against the target security controls. The **Issuing-CAs** is also subject to regular surveillance audits from the PMA.

6.5.4 Computer Security Rating

The technical aspects of computer security are subject to periodic audits.

6.6 Life Cycle Technical Controls

6.6.3 System Development Controls

Purchased hardware or software are shipped in a sealed, tamper-proof container, and installed by qualified personnel. Hardware and software updates are procured in the same manner as the original equipment. Dedicated hardware and software are used for performing CA activities and there are no deployed components that are not part of the CA operations. Dedicated trusted personnel are involved in implementing the required **Issuing-CAs** configuration according to documented operational procedures.

The **Issuing-CAs** hardware and software are tested, deployed and configured 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 operations team.

All **Issuing-CAs** hardware and software platforms are hardened using industry best practices and vendor recommendations.

6.6.4 Security Management Controls

The hardware and software used to set up the **Issuing-CAs** 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.

A configuration management process is enforced to ensure that the **Issuing-CAs** systems configuration, modification and upgrades are documented and controlled by the PKI operations management.

A vulnerability management process is enforced to ensure that the **Issuing-CAs** equipment is scanned for malicious code on first use and periodically thereafter. The vulnerability management process supports the processing within 96 hours of discovery of critical vulnerabilities not previously met by the operations team.

6.6.5 Life-Cycle Security Controls

Refer to 6.5.1.

6.7 Network security controls

The AGCE implemented strong network security, including managed firewalls and intrusion detection systems.

The network is segmented into several zones, based on their functional, logical and physical relationship. Network boundaries is applied to limit the communication between systems (within zones) and communication between zones, with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations, disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

Issuing Systems, Certificate Management Systems, and Security Support Systems are protected within a highly Secure Network Zone.

The AGCE PKI GB ensures regular vulnerability testing is conducted on the **Issuing-CAs** online services. The AGCE PKI GB also ensures that at least once a year, penetration testing is conducted on the **Issuing-CAs** connected systems, by an independent third-party.

6.8 Time-stamping

The **Issuing-CAs** components are regularly synchronized with a reliable time service. AGCE operates a Timestamping Authority (TSA) and uses its GPS NTP server for time synchronization and to establish the correct time for:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates;
- Issuance of Subscriber end entity Certificates.

6.8.3 Code Signing Timestamping Services

As part of its certification services, the AGCE operates a Time-stamping Authority (TSA) service in accordance with ETSI TS 102 023 “Policy requirements for time-stamping authorities” and ETSI TS 101 861 “Time Stamping Profile” with regard to the time-stamping profile. The AGCE Timestamping signing certificate is issued by the AGCE Trust Services CA. The AGCE Timestamping Policy and Practice Statement specifies the policy requirements relating to the operation of AGCE Time-stamping Authority (TSA). It shall be read in conjunction with this CP/CPS. All documents can be downloaded from <https://ca.pki.agce.dz/repository>.

All Digital Signatures created by Code Signing certificates issued by the Code Signing CA have the ability to include a trusted timestamp issued from the AGCE Trust Services CA.

7. Certificates, CRL, and OCSP Profiles

7.1 Certificate Profile

The **Issuing-CAs** meets the technical requirements set forth in Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking of the CA/Browser Baseline Requirements.

The **Issuing-CAs** generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.3 Version number(s)

X.509 v3 is supported and used for all certificates related to the **Issuing-CAs**.

7.1.4 Certificate extensions

X.509 v3 extensions are supported and used in alignment with the CA/B Forum Baseline Requirements sections 7.1. Refer to sections 7.1.10 and 7.1.11 of this CPS for the details of the contents of the certificates issued by the **Issuing-CAs**.

7.1.5 Algorithm object identifiers

“SHA-256 with RSA” algorithm (OID = {1 2 840 113549 1 1 11}) is used by the **Issuing-CAs**.

7.1.6 Name forms

Name forms in the certificates issued by the **Issuing-CAs** are specified in Section 3.1.1. Refer to sections 7.1.10 and 7.1.11 of this CPS for the certificates contents details.

7.1.7 Name constraints

Name constraints extension is not supported.

7.1.8 Certificate policy object identifier

Certificate policy object identifiers are used as an OID scheme specified for the Algeria National PKI. per RFC 3739 and RFC 5280. Refer to sections 7.1.10 and 7.1.11 of this CPS for the details of the contents of the certificates issued by the Issuing CAs including the values of the OID identifiers.

7.1.9 Usage of Policy Constraints extension

Policy Constraints extension is not supported.

7.1.10 Policy qualifiers syntax and semantics

The use of policy qualifiers defined in RFC 5280 is supported. Refer to sections 7.1.10 and 7.1.11 of this CPS for the details of the contents of the certificates issued by the **Issuing-CAs** including the values of the policy qualifiers.

7.1.11 Processing semantics for the critical Certificate Policies extension

Certificate policies extensions must be processed as per RFC 5280.

7.1.12 Certificates for natural persons

7.1.12.1 Qualified Signing Certificate Profile

CE² = Critical Extension
Static, D = Dynamic

O/M³: O = Optional M = Mandatory

CO⁴ = Content: S =

| Qualified Signing Certificate Profile | | | | | |
|---------------------------------------|-----------------|------------------|-----------------|-----------------------------|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | Corporate CA Signature. | Corporate CA's signature value |
| TBSCertificate | | | | | |
| Version | False | M | S | | |
| Version | | M | S | 2 | Version 3 |
| SerialNumber | False | M | D | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |

| | | | | | |
|---------------------|-------|-----|---|---|--|
| | | | | | |
| Issuer | False | M | S | <Issuing CA's Subject> | The issuer field is defined as the X.501 type "Name" |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTAL E DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| CommonName | | M | S | Corporate CA | UTF8 encoded |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| NotBefore | | M | D | Certificate generation process date/time. | |
| NotAfter | | M | D | Certificate generation process date/time + up to [36] Months | Suggested validity for the end user certificate is up to 3 years |
| Subject | False | | | | |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | D | Organization name of a legal entity associated with the natural person | UTF8 encoded |
| OrganizationUnit | | O | D | Organizational unit name within a legal entity associated with the natural person | UTF8 encoded |
| localityName | | M/O | D | Government entity locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not |

| | | | | | |
|------------------------|-------|---|---|--|--|
| | | | | | present, optional if the localityName is present. |
| CommonName | | M | D | Concatenation of given name and surname as in government-issued ID card separated by a “space” character | UTF8 encoded |
| SERIALNUMBER | | M | D | <Unique employee Identifier or Unique National Identifier as agreed between the subscriber and the LRAO> | PrintableString encoded |
| GivenName | | O | D | Given name of the individual (must be present if Surname is present) | UTF8 encoded |
| Surname | | O | D | Surname name of the individual (must be present if GivenName is present) | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | RSA / ECDSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA) | |
| Extensions | | | | | |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 Hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| AuthorityInfoAccess | False | M | S | | |
| AccessMethod | | M | S | <i>Id-ad-2 1 id-ad-ocsp OID i.e., 1.3.6.1.5.5.7.48.1 (ca ocsp)</i> | OCSP Responder field |
| AccessLocation | | M | S | http://ocsp.pki.agce.dz | OCSP responder URL |

| | | | | | | |
|--|------------------------------------|-------|---|---|---|--|
| | AccessMethod | | M | S | <i>Id-ad-2 2 id-ad-caIssuers OID i.e., 1.3.6.1.5.5.7.48.2 (ca cert)</i> | CA Issuers field |
| | AccessLocation | | M | S | http://ca.pki.agce.dz/repository/cert/corporate_ca_1.p7b | Issuing CA Certificate/Chain download URL over HTTP |
| | crlDistributionPoints | False | M | S | | |
| | DistributionPoint | | M | S | http://ca.pki.agce.dz/repository/crl/corporate_ca_crl | CRL download URL. |
| | Subject Properties | | | | | |
| | SubjectKeyIdentifier | False | M | D | | |
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| | Key Usage Properties | | | | | |
| | keyUsage | True | M | S | | |
| | nonrepudiation | | M | S | True | |
| | Policy Properties | | | | | |
| | Certificate Policies | False | M | S | | |
| | PolicyIdentifier | | M | S | 2.16.12.3.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | S | https://ca.pki.agce.dz/repository/cps | |
| | Certificate Policies | False | M | S | | |
| | PolicyIdentifier | | M | S | 2.16.12.3.1.3.1.2 in case of certificates generated on tokens or 2.16.12.3.1.3.1.5 in case of remote signing certificates | |

7.1.12.2 Advanced Signing Certificate Profile

CE² = Critical Extension
Static, D = Dynamic

O/M³: O = Optional M = Mandatory

CO⁴ = Content: S =

| Advanced Signing Certificate Profile | | | | | |
|--------------------------------------|-----------------|------------------|-----------------|---|---|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | Issuing CA's Signature. | Corporate CA signature value |
| TBSCertificate | | | | | |
| Version | False | M | S | | |
| Version | | M | S | 2 | Version 3 |
| SerialNumber | False | M | D | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | < Issuing CA's Subject > | The issuer field is defined as the X.501 type "Name" |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTAL E DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| CommonName | | M | S | Corporate CA | UTF8 encoded |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |

| | | | | | | |
|--|---------------------|-------|-----|---|--|--|
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + up to [36] Months | Suggested validity for the end user certificate is up to 3 years |
| | Subject | False | | | | |
| | CountryName | | M | S | DZ | Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280) |
| | OrganizationName | | M | D | Organization name of a legal entity associated with the natural person | UTF8 encoded |
| | OrganizationUnit | | O | D | Organizational unit name within a legal entity associated with the natural person | UTF8 encoded |
| | localityName | | M/O | D | Government entity locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| | stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| | CommonName | | M | D | Concatenation of given name and surname as in government-issued ID card separated by a “space” character | UTF8 encoded |
| | SERIALNUMBER | | M | D | < unique employee identifier or unique national identifier as agreed between the LRA and the subscribers > | PrintableString encoded |
| | GivenName | | O | D | Given name of the individual (must be present if Surname is present) | UTF8 encoded |

| | | | | | |
|------------------------|-------|---|---|---|--|
| Surname | | O | D | Surname name of the individual (must be present if GivenName is present) | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | RSA / ECDSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA) | |
| Extensions | | | | | |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 Hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| AuthorityInfoAccess | False | M | S | | |
| AccessMethod | | M | S | <i>Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsf)</i> | OCSP Responder field |
| AccessLocation | | M | S | http://ocsp.pki.agce.dz | OCSP responder URL |
| AccessMethod | | M | S | <i>Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)</i> | CA Issuers field |
| AccessLocation | | M | S | http://ca.pki.agce.dz/repository/cert/corporate_ca_1.p7b | Issuing CA Certificate/Chain download URL over HTTP |
| crlDistributionPoints | False | M | S | | |
| DistributionPoint | | M | S | http://ca.pki.agce.dz/repository/crl/corporate_ca.crl | CRL download URL. |
| Subject Properties | | | | | |
| SubjectKeyIdentifier | False | M | D | | |

| | | | | | | |
|----------------------|------------------------------------|-------|---|---|---|--|
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| Key Usage Properties | | | | | | |
| | keyUsage | True | M | S | | |
| | nonrepudiation | | M | S | True | |
| Policy Properties | | | | | | |
| | Certificate Policies | False | M | S | | |
| | PolicyIdentifier | | M | S | 2.16.12.3.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | S | https://ca.pki.agce.dz/registry/cps | |
| | Certificate Policies | False | M | S | | |
| | PolicyIdentifier | | M | S | 2.16.12.3.1.3.1.3 | |

7.1.12.3 Email protection (SMIME) Certificate Profile

CE² = Critical Extension
Static, D = Dynamic

O/M³: O = Optional M = Mandatory

CO⁴ = Content: S =

| EmailProtection Certificate Profile | | | | | | |
|-------------------------------------|-----------------|------------------|-----------------|-----------------------------|--|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment | |
| Certificate | | M | | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 | |
| Signature | False | M | | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption | |
| SignatureValue | | M | D | Issuing CA's Signature. | Corporate CA's signature value | |
| TBSCertificate | | | | | | |
| Version | False | M | S | | | |
| Version | | M | S | 2 | Version 3 | |
| SerialNumber | False | M | D | | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. | |

| | | | | | | |
|-----------|---------------------|-------|-----|---|--|--|
| Signature | | False | M | S | | |
| | AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | | False | M | S | | |
| | CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| | OrganizationName | | M | S | AUTORITE GOUVERNEMENTAL E DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| | CommonName | | M | S | SMIME CA | UTF8 encoded |
| Validity | | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + up to [810] days | validity for the end user certificate is up to 27 months |
| Subject | | False | | | | |
| | CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| | OrganizationName | | M | D | Organization name of a legal entity associated with the natural person | UTF8 encoded |
| | OrganizationUnit | | O | D | Organizational unit name within a legal entity associated with the natural person | UTF8 encoded |
| | localityName | | M/O | D | Government entity locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the |

| | | | | | |
|------------------------|-------|-----|---|--|--|
| | | | | | stateOrProvinceName is present. |
| stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| CommonName | | M | D | Concatenation of given name and surname as in government-issued ID card separated by a "space" character | UTF8 encoded |
| SERIALNUMBER | | M | D | < unique employee identifier or unique national identifier as agreed between the LRA and the subscribers > | PrintableString encoded |
| GivenName | | O | D | Given name of the individual (must be present if Surname is present) | UTF8 encoded |
| Surname | | O | D | Surname name of the individual (must be present if GivenName is present) | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | RSA / ECDSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA) | |
| Extensions | | | | | |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 Hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| AuthorityInfoAccess | False | M | S | | |

| | | | | | | |
|--|------------------------------------|-------|---|---|---|--|
| | AccessMethod | | M | S | <i>Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsf)</i> | OCSP Responder field |
| | AccessLocation | | M | S | http://ocsp.pki.agce.dz | OCSP responder URL |
| | AccessMethod | | M | S | <i>Id-ad-2 2 id-ad- caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)</i> | CA Issuers field |
| | AccessLocation | | M | S | http://ca.pki.agce.dz/ repository/cert/smime_ca.p 7b | Issuing CA Certificate/Chain download URL over HTTP |
| | crlDistributionPoints | False | M | S | | |
| | DistributionPoint | | M | S | http://ca.pki.agce.dz/ repository/crl/smime_ca.c rl | CRL download URL. |
| | Subject Properties | | | | | |
| | SubjectKeyIdentifier | False | M | D | | |
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| | Subject Alternative Name | False | M | D | | |
| | rfc822Name | | M | D | <email ID> | |
| | Key Usage Properties | | | | | |
| | keyUsage | True | M | S | | |
| | digitalSignature | | M | S | True | |
| | keyEncipherment | | M | S | True | |
| | Extended Key Usage | False | M | S | | |
| | id-kp-emailProtection | | M | S | True | |
| | Policy Properties | | | | | |
| | Certificate Policies | False | M | | | |
| | PolicyIdentifier | | M | S | 2.16.12.3.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |

| | | | | | |
|-----------------------------------|-------|---|---|---|-------------------|
| policyQualifiers:qualifier:cPSuri | | M | S | https://ca.pki.agce.dz/repository/cps | |
| Certificate Policies | False | M | | | |
| PolicyIdentifier | | M | S | 2.16.12.3.1.3.1.4 | SMIME profile OID |

7.1.12.4 Authentication Certificate Profile

CE² = Critical Extension
Static, D = Dynamic

O/M³: O = Optional M = Mandatory

CO⁴ = Content: S =

| Authentication Certificate Profile | | | | | |
|------------------------------------|-----------------|------------------|-----------------|------------------------------------|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | Issuing CA's Signature. | Corporate CA's signature value |
| TBSCertificate | | | | | |
| Version | False | M | S | | |
| Version | | M | S | 2 | Version 3 |
| SerialNumber | False | M | D | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTAL E DE | UTF8 encoded |

| | | | | | |
|---------------------|-------|-----|---|--|--|
| | | | | CERTIFICATION ELECTRONIQUE | |
| CommonName | | M | S | Corporate CA | UTF8 encoded |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using Generalised Time |
| NotBefore | | M | D | Certificate generation process date/time. | |
| NotAfter | | M | D | Certificate generation process date/time + up to [36] Months | Suggested validity for the end user certificate is up to 3 years |
| Subject | False | | | | |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | D | Organization name of a legal entity associated with the natural person | UTF8 encoded |
| OrganizationUnit | | O | D | Organizational unit name within a legal entity associated with the natural person | UTF8 encoded |
| localityName | | M/O | D | Government entity locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| CommonName | | M | D | Concatenation of given name and surname as in government-issued ID card separated by a "space" character | UTF8 encoded |
| SERIALNUMBER | | M | D | < unique employee identifier or unique national identifier as agreed between the | PrintableString encoded |

| | | | | | |
|------------------------|-------|---|---|---|--|
| | | | | LRA and the subscribers > | |
| GivenName | | O | D | Given name of the individual (must be present if Surname is present) | UTF8 encoded |
| Surname | | O | D | Surname name of the individual (must be present if GivenName is present) | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | RSA / ECDSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA) | |
| Extensions | | | | | |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 Hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| AuthorityInfoAccess | False | M | S | | |
| AccessMethod | | M | S | <i>Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsf)</i> | OCSP Responder field |
| AccessLocation | | M | S | http://ocsp.pki.agce.dz | OCSP responder URL |
| AccessMethod | | M | S | <i>Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)</i> | CA Issuers field |
| AccessLocation | | M | S | http://ca.pki.agce.dz/repository/cert/corporate_ca_1.p7b | Issuing CA Certificate/Chain download URL over HTTP |
| crIDistributionPoints | False | M | S | | |

| | | | | | | |
|----------------------|------------------------------------|-------|---|---|---|--|
| | DistributionPoint | | M | S | http://ca.pki.agce.dz/repository/crl/corporate_ca.crl | CRL download URL. |
| Subject Properties | | | | | | |
| | SubjectKeyIdentifier | False | M | D | | |
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| Key Usage Properties | | | | | | |
| | keyUsage | True | M | S | | |
| | digitalSignature | | M | S | True | |
| Extended Key Usage | | | | | | |
| | id-kp-clientAuth | False | M | S | True | |
| Policy Properties | | | | | | |
| Certificate Policies | | | | | | |
| | PolicyIdentifier | False | M | S | 2.16.12.3.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | S | https://ca.pki.agce.dz/repository/cps | |
| Certificate Policies | | | | | | |
| | PolicyIdentifier | False | M | S | 2.16.12.3.1.3.1.1 | |

7.1.13 Certificates for legal persons

7.1.13.1eSeal Certificate Profile

CE² = Critical Extension O/M³: O = Optional M = Mandatory CO⁴ = Content: S = Static, D = Dynamic

| eSeal Certificate Profile | | | | | | |
|---------------------------|-----------------|------------------|-----------------|-----------------------------|----------------------------|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment | |
| Certificate | | M | | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 | |
| Signature | False | M | | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption | |

| | | | | | | |
|--|-------------------------|-------|---|---|---|--|
| | SignatureValue | | M | D | Issuing CA's Signature. | Corporate CA's signature value |
| | | | | | | |
| | Version | False | M | S | | |
| | Version | | M | S | 2 | Version 3 |
| | SerialNumber | False | M | D | | |
| | CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| | Signature | False | M | S | | |
| | AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| | Issuer | False | M | S | < Issuing CA's Subject > | The issuer field is defined as the X.501 type "Name" |
| | CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| | OrganizationName | | M | S | AUTORITE GOUVERNEMENTAL E DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| | CommonName | | M | S | Corporate CA | UTF8 encoded |
| | Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + up to [36] Months | Suggested validity for the end user certificate is up to 3 years |
| | Subject | False | | | | |
| | CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |

| | | | | | |
|------------------------|-------|-----|---|---|--|
| OrganizationName | | M | D | Full registered name of organization to which the certificate is issued | UTF8 encoded |
| OrganizationUnit | | O | D | Organizational unit name within the legal entity | UTF8 encoded |
| localityName | | M/O | D | Government entity locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| CommonName | | M | D | Contains the full organization registered name | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | RSA / ECDSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) / 256, 384 or 521 (ECDSA) | |
| Extensions | | | | | |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 Hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| AuthorityInfoAccess | False | M | S | | |
| AccessMethod | | M | S | <i>Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)</i> | OCSP Responder field |
| AccessLocation | | M | S | http://ocsp.pki.agce.dz | OCSP responder URL |

| | | | | | |
|------------------------------------|-------|---|---|---|--|
| AccessMethod | | M | S | <i>Id-ad-2.2 id-ad-caIssuers OID i.e., 1.3.6.1.5.5.7.48.2 (ca cert)</i> | CA Issuers field |
| AccessLocation | | M | S | http://ca.pki.agce.dz/repository/cert/corporate_ca_1.p7b | Issuing CA Certificate/Chain download URL over HTTP |
| crlDistributionPoints | False | M | S | | |
| DistributionPoint | | M | S | http://ca.pki.agce.dz/repository/crl/corporate_ca.crl | CRL download URL. |
| Subject Properties | | | | | |
| SubjectKeyIdentifier | False | M | D | | |
| KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| Key Usage Properties | | | | | |
| keyUsage | True | M | S | | |
| digitalSignature | | M | S | True | |
| Policy Properties | | | | | |
| Certificate Policies | False | M | S | | |
| PolicyIdentifier | | M | S | 2.16.12.3.2.1.2 | |
| policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| policyQualifiers:qualifier:cPSuri | | M | S | https://ca.pki.agce.dz/repository/cps | |
| Certificate Policies | False | M | S | | |
| PolicyIdentifier | | M | S | 2.16.12.3.1.3.2.1 | |

7.1.13.2 Code Signing Certificate Profile

CE² = Critical Extension
Static, D = Dynamic

O/M³: O = Optional M = Mandatory

CO⁴ = Content: S =

| Code Signing Certificate Profile | | | | | |
|----------------------------------|-----------------|------------------|-----------------|-------|---------|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |

| | | | | | | |
|------------------|-------------------------|-------|---|---|---|---|
| TBSCertificate | | | M | | | See 4.1.2 of RFC 5280 |
| Signature | | False | M | | | |
| | AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| | SignatureValue | | M | D | Issuing CA's Signature. | Corporate CA's signature value |
| TBSCertificate | | | | | | |
| Version | | False | M | S | | |
| | Version | | M | S | 2 | Version 3 |
| SerialNumber | | False | M | D | | |
| | CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| Signature | | False | M | S | | |
| | AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | | False | M | S | < Issuing CA's Subject> | The issuer field is defined as the X.501 type "Name" |
| CountryName | | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | | M | S | AUTORITE GOUVERNEMENTAL E DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| CommonName | | | M | S | Code Signing CA | UTF8 encoded |
| Validity | | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + [36] Months | Suggested validity for the end user certificate is 3 years |

| | | | | | |
|------------------------|-------|-----|---|---|--|
| Subject | False | | | | |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | D | Full registered name of organization to which the certificate is issued | UTF8 encoded |
| OrganizationUnit | | O | D | Organizational unit name within the legal entity | UTF8 encoded |
| localityName | | M/O | D | Government entity locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| CommonName | | M | D | Contains the full organization registered name | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | RSA / ECDSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 3072 or 4096 (RSA) / 256, 384 or 521 (ECDSA) | |
| Extensions | | | | | |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 Hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| AuthorityInfoAccess | False | M | S | | |

| | | | | | | |
|--|------------------------------------|-------|---|---|---|--|
| | AccessMethod | | M | S | <i>Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsf)</i> | OCSP Responder field |
| | AccessLocation | | M | S | http://ocsp.pki.agce.dz | OCSP responder URL |
| | AccessMethod | | M | S | <i>Id-ad-2 2 id-ad- caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)</i> | CA Issuers field |
| | AccessLocation | | M | S | http://ca.pki.agce.dz/re pository/cert/code- signing_ca.p7b | Issuing CA Certificate/Chain download URL over HTTP |
| | crlDistributionPoints | False | M | S | | |
| | DistributionPoint | | M | S | http://ca.pki.agce.dz/re pository/crl/code- signing_ca.crl | CRL download URL. |
| | Subject Properties | | | | | |
| | SubjectKeyIdentifier | False | M | D | | |
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| | Key Usage Properties | | | | | |
| | keyUsage | True | M | S | | |
| | digitalSignature | | M | S | True | |
| | Extended Key Usage | False | M | S | | |
| | id-kp-codeSigning | | M | S | True | |
| | Policy Properties | | | | | |
| | Certificate Policies | False | M | | | |
| | PolicyIdentifier | | M | S | 2.16.12.3.2.1.2 | Corporate CAs CPS |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | S | https://ca.pki.agce.dz/re pository/cps | |
| | Certificate Policies | False | M | | | |
| | PolicyIdentifier | | M | S | 2.23.140.1.4.1 | BR CS Reserved OID |

| | | | | | |
|----------------------|-------|---|---|-------------------|--|
| Certificate Policies | False | M | S | | |
| PolicyIdentifier | | M | S | 2.16.12.3.1.3.2.2 | |

7.2 CRL Profile

In conformance with the IETF PKIX RFC 5280, the **Issuing-CAs** supports CRLs compliant with:

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

7.2.3 Issuing CAs CRL

The **Issuing-CAs** CRL is as follows:

CE² = Critical Extension O/M³: O = Optional M = Mandatory CO⁴ = Content: S = Static, D = Dynamic

7.2.3.1 Corporate CA CRL Profile

| Corporate CA CRL Profile | | | | | |
|--------------------------|-----------------|------------------|-----------------|------------------------------|--------------------------------|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| CertificateList | | M | | | |
| TBSCertificate | | | | | |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | CA's Signature. | Corporate CA's signature value |
| TbSCertList | | | | | |
| Version | False | M | S | | |
| Version | | | S | 1 | Version 2 |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| CountryName | | M | S | DZ | |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTAL E DE | |

| | | | | CERTIFICATION ELECTRONIQUE | |
|-------------------------|--|-------|---|----------------------------|--|
| CommonName | | M | S | Corporate CA | |
| Validity | | False | M | D | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| thisUpdate | | | M | D | <creation time> |
| NextUpdate | | | M | D | <Creation time> + [1] day + 2 hours |
| RevokedCertificates | | False | O | D | |
| Certificate | | | M | D | |
| CertificateSerialNumber | | | M | D | Serial of the revoked certificates |
| revocationDate | | | M | D | Date when revocation was processed by the CA UTC time of revocation |
| crlEntryExtension | | False | O | D | |
| CRLReason | | | O | D | As per RFC 5280 Identifies the reason for the certificate revocation |
| Invalidity Date | | | O | D | Date when the certificate is supposed to be invalid Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| CRLExtensions | | False | M | D | |
| AuthorityKeyIdentifier | | False | M | D | 160-bit SHA-1 hash of the Corporate CA public key |
| CRL Number | | False | M | D | Sequential CRL Number |
| expiredCertsOnCRL | | False | M | D | < a date-time value specifies the date on or after which revoked certificates are retained on the CRL> |
| AuthorityInfoAccess | | False | O | S | |
| AccessMethod | | | O | S | <i>Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)</i> CA Issuers field |

| | | | | | |
|----------------|--|---|---|---|---|
| AccessLocation | | O | S | http://ca.pki.agce.dz/repository/cert/corporate_ca_1.p7b | Issuing CA Certificate/Chain download URL over HTTP |
|----------------|--|---|---|---|---|

7.2.3.2 Code Signing CA CRL Profile

| Code Signing CA CRL Profile | | | | | |
|-----------------------------|-----------------|------------------|-----------------|--|---|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| CertificateList | | M | | | |
| TBSCertificate | | | | | |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | CA's Signature. | Corporate CA's signature value |
| TbSCertList | | | | | |
| Version | False | M | S | | |
| Version | | | S | 1 | Version 2 |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| CountryName | | M | S | DZ | |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | |
| CommonName | | M | S | Code Signing CA | |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| thisUpdate | | M | D | <creation time> | |

| | | | | | | |
|--|-------------------------|-------|---|---|---|--|
| | NextUpdate | | M | D | <Creation time> + [1] day + 2 hours | |
| | RevokedCertificates | False | O | D | | |
| | Certificate | | M | D | | |
| | CertificateSerialNumber | | M | D | Serial of the revoked certificates | |
| | revocationDate | | M | D | Date when revocation was processed by the CA | UTC time of revocation |
| | crlEntryExtension | False | O | D | | |
| | CRLReason | | O | D | As per RFC 5280 | Identifies the reason for the certificate revocation |
| | Invalidity Date | | O | D | Date when the certificate is supposed to be invalid | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| | CRLExtensions | False | M | D | | |
| | AuthorityKeyIdentifier | False | M | D | 160-bit SHA-1 hash of the Code Signing CA public key | |
| | CRL Number | False | M | D | | Sequential CRL Number |
| | expiredCertsOnCRL | False | M | D | | < a date-time value specifies the date on or after which revoked certificates are retained on the CRL> |
| | AuthorityInfoAccess | False | O | S | | |
| | AccessMethod | | O | S | Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert) | CA Issuers field |
| | AccessLocation | | O | S | http://ca.pki.agce.dz/repository/cert/code-signing_ca.p7b | Issuing CA Certificate/Chain download URL over HTTP |

7.2.3.3 SMIME CA CRL Profile

| SMIME CA CRL Profile | | | | | |
|----------------------|-----------------|------------------|-----------------|---|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| CertificateList | | M | | | |
| TBSCertificate | | | | | |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | CA's Signature. | Corporate CA's signature value |
| TbSCertList | | | | | |
| Version | False | M | S | | |
| Version | | | S | 1 | Version 2 |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| CountryName | | M | S | DZ | |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | |
| CommonName | | M | S | SMIME CA | |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| thisUpdate | | M | D | <creation time> | |
| NextUpdate | | M | D | <Creation time> + [1] day + 2 hours | |
| RevokedCertificates | False | O | D | | |

| Certificate | | | M | D | | |
|-------------|-------------------------|-------|---|---|---|--|
| | CertificateSerialNumber | | M | D | Serial of the revoked certificates | |
| | revocationDate | | M | D | Date when revocation was processed by the CA | UTC time of revocation |
| | crEntryExtension | False | O | D | | |
| | CRLReason | | O | D | As per RFC 5280 | Identifies the reason for the certificate revocation |
| | Invalidity Date | | O | D | Date when the certificate is supposed to be invalid | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| | CRLExtensions | False | M | D | | |
| | AuthorityKeyIdentifier | False | M | D | 160-bit SHA-1 hash of the SMIME CA public key | |
| | CRL Number | False | M | D | | Sequential CRL Number |
| | expiredCertsOnCRL | False | M | D | | < a date-time value specifies the date on or after which revoked certificates are retained on the CRL> |
| | AuthorityInfoAccess | False | O | S | | |
| | AccessMethod | | O | S | Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert) | CA Issuers field |
| | AccessLocation | | O | S | http://ca.pki.agce.dz/repository/cert/smime_ca.p7b | Issuing CA Certificate/Chain download URL over HTTP |

7.2.4 Version number(s)

The **Issuing-CAs** supports X.509 version 2 CRLs (see 7.2 above)

7.2.5 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.

7.3.3 Issuing CAs OCSP

7.3.3.1 Corporate OCSP Response Signing Certificate Profile

The **Issuing-CAs** OCSP response signing certificate profile is as follows:

CE² = Critical Extension
Static, D = Dynamic

O/M³: O = Optional M = Mandatory

CO⁴ = Content: S =

| Corporate CA OCSP Response Signing Certificate Profile | | | | | |
|--|-----------------|------------------|-----------------|--------------------------------|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | CA's Signature. | CA's signature value |
| TBSCertificate | | | | | |
| Version | False | M | S | | |
| Version | | M | S | 2 | Version 3 |
| SerialNumber | False | M | S | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | < Issuing CA's Subject > | The issuer field is defined as the X.501 type "Name" |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |

| | | | | | |
|----------------------|-------|---|---|---|--|
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| CommonName | | M | S | Corporate CA | UTF8 encoded |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| NotBefore | | M | D | Certificate generation process date/time. | |
| NotAfter | | M | D | Certificate generation process date/time + [12] Months | Suggested validity for the OCSP certificate is one year |
| Subject | False | M | S | | |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| stateOrProvinceName | | M | S | Algiers | UTF8 encoded. |
| CommonName | | M | S | Corporate CA OCSP | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | | | |
| AlgorithmIdentifier | | M | S | RSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) | |
| Extensions | | M | | | |
| Subject Properties | | | | | |
| SubjectKeyIdentifier | False | M | D | | |
| KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |

| | | | | | |
|------------------------|-------|---|---|---|--|
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 hash of the Corporate CA public key | When this extension is used, this field MUST be supported as a minimum |
| Policy Properties | | | | | |
| keyUsage | True | M | S | | |
| digitalSignature | | M | S | True | |
| extKeyUsage | False | M | S | | |
| id-kp-OCSPSigning | | M | S | True | |
| id-pkix-ocsp-nocheck | False | M | S | | |
| basicConstraints | True | O | S | False | |

7.3.3.2 Code Signing OCSP Response Signing Certificate Profile

| Code Signing CA OCSP Response Signing Certificate Profile | | | | | |
|---|-----------------|------------------|-----------------|-----------------------------|--|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | CA's Signature. | CA's signature value |
| TBSCertificate | | | | | |
| Version | False | M | S | | |
| Version | | M | S | 2 | Version 3 |
| SerialNumber | False | M | S | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |

| | | | | | |
|---------------------|-------|---|---|---|--|
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | < Issuing CA's Subject> | The issuer field is defined as the X.501 type "Name" |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| CommonName | | M | S | Code Signing CA | UTF8 encoded |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| NotBefore | | M | D | Certificate generation process date/time. | |
| NotAfter | | M | D | Certificate generation process date/time + [12] Months | Suggested validity for the OCSP certificate is one year |
| Subject | False | M | S | | |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| stateOrProvinceName | | M | S | Algiers | UTF8 encoded. |

| | | | | | |
|------------------------|-------|---|---|--|---|
| CommonName | | M | S | Code Signing CA OCSP | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | | | |
| AlgorithmIdentifier | | M | S | RSA | |
| SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) | |
| Extensions | | M | | | |
| Subject Properties | | | | | |
| SubjectKeyIdentifier | False | M | D | | |
| KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| Authority Properties | | | | | |
| AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| KeyIdentifier | | M | D | 160-bit SHA-1 hash of the Code Signing CA public key | When this extension is used, this field MUST be supported as a minimum |
| Policy Properties | | | | | |
| keyUsage | True | M | S | | |
| digitalSignature | | M | S | True | |
| extKeyUsage | False | M | S | | |
| id-kp-OCSPSigning | | M | S | True | |
| basicConstraints | True | O | S | False | |
| id-pkix-ocsp-nocheck | False | M | S | | |

7.3.3.3 SMIME CA OCSP Response Signing Certificate Profile

| SMIME CA OCSP Response Signing Certificate Profile | | | | | |
|--|-----------------|------------------|-----------------|-------|---------|
| Field | CE ² | O/M ³ | CO ⁴ | Value | Comment |
| Certificate | | M | | | |

| | | | | | |
|-------------------------|-------|---|---|--|--|
| TBSCertificate | | M | | | See 4.1.2 of RFC 5280 |
| Signature | False | M | | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| SignatureValue | | M | D | CA's Signature. | CA's signature value |
| TBSCertificate | | | | | |
| Version | False | M | S | | |
| Version | | M | S | 2 | Version 3 |
| SerialNumber | False | M | S | | |
| CertificateSerialNumber | | M | D | | At least 64 bits of entropy validated on duplicates. |
| Signature | False | M | S | | |
| AlgorithmIdentifier | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | < Issuing CA's Subject> | The issuer field is defined as the X.501 type "Name" |
| CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| CommonName | | M | S | SMIME CA | UTF8 encoded |
| Validity | False | M | D | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |

| | | | | | | |
|--|------------------------|-------|---|---|--|--|
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + [12] Months | Suggested validity for the OCSP certificate is one year |
| | Subject | False | M | S | | |
| | CountryName | | M | S | DZ | Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) |
| | OrganizationName | | M | S | AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE | UTF8 encoded |
| | stateOrProvinceName | | M | S | Algiers | UTF8 encoded. |
| | CommonName | | M | S | SMIME CA OCSP | UTF8 encoded |
| | SubjectPublicKeyInfo | False | M | | | |
| | AlgorithmIdentifier | | M | S | RSA | |
| | SubjectPublicKey | | M | D | Public Key Key length: 2048 or 4096 (RSA) | |
| | Extensions | | M | | | |
| | Subject Properties | | | | | |
| | SubjectKeyIdentifier | False | M | D | | |
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of SubjectPublicKey | When this extension is used, this field MUST be supported as a minimum |
| | Authority Properties | | | | | |
| | AuthorityKeyIdentifier | False | M | D | | Mandatory in all certificates except for self-signed certificates |
| | KeyIdentifier | | M | D | 160-bit SHA-1 hash of the SMIME CA public key | When this extension is used, this field |

| | | | | | |
|----------------------|-------|---|---|-------|--------------------------------|
| | | | | | MUST be supported as a minimum |
| Policy Properties | | | | | |
| keyUsage | True | M | S | | |
| digitalSignature | | M | S | True | |
| extKeyUsage | False | M | S | | |
| id-kp-OCSPSigning | | M | S | True | |
| id-pkix-ocsp-nocheck | False | M | S | | |
| basicConstraints | True | O | S | False | |

7.3.4 Version number(s)

As per the OCSP certificate profile, section 7.3.

7.3.5 OCSP extensions

As per the OCSP certificate profile, section 7.3.

8. Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

The AGCE PKI GB ensures that the **Issuing-CAs** operations are subject to regular internal audits. These audits are planned and executed, at a minimum, once yearly 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 in coordination with the PMA and apply for the GOV-CA operations as well as to the **Issuing-CAs**. AGCE accepts this auditing of its own practices and procedures and will make the audit report publicly available no later than three months after the end of the audit period. The PKI GB evaluates the results of such audits before further implementing them.

The AGCE compliance function executes yearly verifications on LRA organizations to verify that personnel (LRAOs) involved in verification duties and related certificate issuance comply with the provisions listed in this CPS.

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

The external auditor shall be an independent auditor appointed who will not be affiliated directly or indirectly in any way with AGCE nor any person having any conflicting interests thereof.

8.4 Topics covered by assessment

The **Corporate CA**, **SMIME CA** are audited for compliance to the following standards

- WebTrust for Certification Authorities Principles And Criteria

The **Code Signing CA** is audited for compliance to the following standards

- WebTrust for Certification Authorities Principles And Criteria
- 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 sufficiently 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-authorized third parties.

External audits are published on the **AGCE** repository.

8.7 Self-audits

The AGCE, through its compliance function, monitors and strictly controls its adherence to the procedures listed in this CPS document by performing self-audits on at least a quarterly basis against a randomly selected samples at least 3 percent of the Certificates issued by the **Issuing-CAs**.

Refer to sections 8.1 and 8.6 for other internal audits performed on the **Issuing-CAs** operations.

9. Other Business and Legal Matters

9.1 Fees

9.1.3 Certificate Issuance or Renewal Fees

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

9.1.4 Certificate Access Fees

Not applicable.

9.1.5 Revocation or Status Information Access Fees

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

9.1.6 Fees for Other Services

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

9.1.7 Refund Policy

No refunds for any charged fees.

9.2 Financial Responsibility

9.2.3 Insurance coverage

The AGCE PKI GB ensures that the **Issuing-CAs** is covered by existing government insurance provisions.

9.2.4 Other assets

The AGCE PKI GB maintains sufficient financial resources to support the continuous operations of the **Issuing-CAs** and ensure the fulfilment of the **Issuing-CAs** duties as per the provisions of this CPS.

9.2.5 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.3 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 **Issuing-CAs**;
- Correspondence between the subscribers and the AGCE RA / LRAs 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.

9.3.4 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.

9.3.5 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

9.4.3 Privacy plan

The AGCE observes personal data privacy rules and privacy rules as specified in the present CPS. The AGCE implements these provisions through the AGCE RA and LRAs.

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 except for information about themselves and only covered by the contractual agreement between the AGCE and the subscribers.

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 **Issuing-CAs** systems. This shall include:

- The communications between the AGCE RA/LRA systems and the subscribers;
- The communications between the LRA and the **Issuing-CAs** systems;
- Sessions to deliver certificates.

9.4.4 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.

9.4.5 Information not Deemed Private

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

9.4.6 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.

9.4.7 Notice and consent to use private information

The AGCE ensure 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 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.

9.4.8 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.

9.4.9 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 **Issuing-CAs** databases, repository, the **Issuing-CAs** digital certificates and any other publication originating from the PKI GB, including this CPS.

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

9.6 Representations and Warranties

9.6.3 CA Representations and Warranties

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

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

The AGCE represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the **Issuing-CAs** has complied with the Baseline Requirements and its CPS in issuing and managing the Certificate.

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

- **Authorization for Certificate:** That, at the time of issuance, the **Issuing-CAs** (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 this CPS;
- **Accuracy of Information:** That, at the time of issuance, the **Issuing-CAs** (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 this CPS;
- **No Misleading Information:** That, at the time of issuance, the **Issuing-CAs** (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 this CPS;
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the **Issuing-CAs** (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 this CPS;
- **Subscriber Agreement:** That, if the **Issuing-CAs** 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 **Issuing-CAs** maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;

- **Revocation:** That the **Issuing-CAs** will revoke the Certificate for any of the reasons specified in these Requirements

9.6.4 RA Representations and Warranties

The AGCE warrants that it performs RA functions as per the stipulations specified in this CPS. The LRAs warrant (through signing an LRA agreement with AGCE) that they perform RA functions as per the stipulations specified in this CPS.

9.6.5 Subscriber Representations and Warranties

The AGCE/LRAs require, as part of the Subscriber Agreement or Terms of Use, that the Applicant makes the commitments and warranties in this section for the benefit of the **Issuing-CAs** 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 /LRA, or

The Applicant's acknowledgement of the Terms of Use.

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

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the AGCE/LRA, both in the certificate request and as otherwise requested by AGCE/LRA in connection with the issuance of the Certificate(s) to be supplied by the **Issuing-CAs** ;
- **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:** When natural or legal person certificates are requested, an obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- **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'/LRA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the AGCE/LRA 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 Corporate CA CPS, or the Baseline Requirements.

9.6.6 Relying parties Representations and Warranties

Relying Parties who rely upon the certificates issued under the **Issuing-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.

9.6.7 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 **Issuing-CAs** with the intention to be included in a certificate;
- indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures;
- willful 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 **Issuing-CAs** services;
- any form of misrepresentation of information by the subscribers or relying parties on information contained in this CPS or any other documentation made public by the AGCE PKI GB and related to the **Issuing-CAs** services.

9.8 Limitations of Liability

Limitations on Liability:

- The **Issuing-CAs** will not incur any liability to the subscribers to the extent that such liability results from their negligence, fraud or willful misconduct;
- The AGCE assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this CPS for any use other than in accordance with this document. Subscribers 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 whatsoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Subscribers and LRAs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by the **Issuing-CAs**;

- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscriber's breach of Subscriber's agreement;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- The AGCE denies any financial or any other kind of responsibility for damages or impairments resulting from the **Issuing-CAs** operation.

9.9 Indemnities

This CPS does not include any claims of indemnity.

9.10 Term and termination

9.10.3 Term

The present CPS is approved by the AGCE PKI GB and shall remain in force until amendments are published on the **Issuing-CAs** repository.

9.10.4 Termination

Amendments to this document are applied and approved by the PKI GB and marked by an indicated new version of the document. Upon publishing on the AGCE repository, the newer version becomes effective. The older versions of this document are archived on the **Issuing-CAs** repository as well.

9.10.5 Effect of Termination and Survival

The PKI GB will communicate the conditions and effect of this CPS termination via appropriate mechanisms.

9.11 Individual notices and communications with participants

Notices related to the present CPS may be addressed by the subscribers/LRAs 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

9.12.3 Procedure for Amendment

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

9.12.4 Notification Mechanism and Period

Upon publishing on the **Issuing-CAs** repository, the newer version of the CPS becomes effective. The older versions of this document are archived on the **Issuing-CAs** repository. The PKI GB coordinates communication towards the relying parties in relation to the amendments of this CPS and related effects.

9.12.5 Circumstances Under Which OID Must Be Changed

Major changes to this CPS that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the OID or qualifier (URL).

9.13 Dispute Resolution Provisions

All disputes associated with the provisions of this CPS and the **Issuing-CAs** 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 CPS.

9.15 Compliance with applicable law

This CPS and provision of **Issuing-CAs** 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*” ;
- *Decret executif N°16-134;*
- *Decret executif N°16-135.*

9.16 Miscellaneous provisions

9.16.3 Entire Agreement

No stipulation.

9.16.4 Assignment

Except where specified by other contracts, no party may assign or delegate rights or duties under this CPS, without the prior written consent of the AGCE.

9.16.5 Severability

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 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 CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.6 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.7 Force Majeure

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

9.17 Other Provisions

Not applicable.

