PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

NATIONAL ELECTRONIC CERTIFICATION AUTHORITY

Algeria National PKI Framework

Certificate Policy for TSPs issuing publicly trusted certificates

Version 3.0

Document Management

Information

Group of document	Algeria National PKI Framework
Title	Certificate Policy for TSPs issuing publicly trusted certificates
Status	Draft
Project reference:	**Algeria National PKI**
Annex:	n.a.

Version control

Version	Date	Description / Status	Responsible
V0.1	14/03/2019	Document preparation	ANCE
V0.2	03/04/2019	Review after March workshop	ANCE
V0.3	18/04/2019	Document update	ANCE
V0.4	07/10/2019	Incorporating latest reviews and updates to accommodate CAB forum vetting procedures updates	ANCE
V0.5	08/12/2019	Latest amendments to accommodate the latest comments from the customer	ANCE
V0.6	19/12/2019	Amending section 3.2	ANCE
V1.0	30/03/2020	Version issued for publishing on PMA/AGCE/AECE web sites	ANCE
V1.1	25/10/2020	Applying final comments from the WebTrust auditor	ANCE
V 1.2	25/09/2021	• Yearly review with changes in wording for more explicit alignment to the Baseline Requirements. • Adding remote signing certificate type in the relevant section. • Alignment of Code signing Key length to latest baseline requirements.	ANCE
V 2.0	01/06/2022	• Major changes following the new Baseline requirements related to Extended Key Usage (EKU) that constraints all Subordinate CAs under the National Root CA. • New Algerian National PKI Hierarchy description • Review/update certificate profiles of Algerian National PKI hierarchy. • Changes to accommodate Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.8.0 which is linked to WebTrust for SSL BR v2.6 • Changes to accommodate Baseline Requirements for the Issuance and Management of Publicly-Trusted Code	ANCE

		Signing Certificates v2.7 which is linked to WebTrust for CS BR v2.7	
V2.1	25/06/2023	• Yearly review and sanity check • Update certificate profiles following the baseline requirements version 2.0.0	ANCE
V3.0	09/05/2024	• New Algerian National PKI Hierarchy description • Review/update certificate profiles of AECE following the new Baseline requirements related to adding Extended Key Usage (EKU) extension • Update the hierarchy of Government Domain CAs following the revocation of the Government SMIME CA and the Code Signing CA • Removal of the certificate profiles for Government SMIME and Code Signing CA following the revocation of both CAs section 7.1 • Adjusting the CRL validity and lifetime for issuing CAs as per the criteria defined in section 4.9.7 of Baseline Requirements for SSL section 2.3.2 • Adding new certificate type profiles for commercial domain in the relevant section • General clean up and minor corrections	ANCE

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V3.0	09/05/2024	ANCE	ANCE (PMA) 22/05/2024	ANCE (PMA) 22/05/2024

References

[RFC 3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[Law 15-04]	Algerian law 15-04 on “signature électronique et certification”, fixant les règles générales relatives à la signature et à la certification électroniques
[Decree 16-134]	Décret exécutif N°16-134 fr
[Decree 16-135]	Décret exécutif N°16-135 fr
AICPA/CPA	Canada Trust Service Principles and Criteria for Certification Authorities
[CABF-BR]	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates

[CABF-NetSec]	CA/B Forum Network and Certificate System Security Requirements
[ANPKI-Supervision]	Algeria National PKI TSP Supervision scheme
[ANPKI-Governance]	Algeria National PKI Governance & Operating model
[ANPKI-TSP-CA CP]	Algeria National PKI TSP-CA certificate policy
[ANPKI-OID]	Algeria National PKI OID structure definition and management
[ANPKI-CT]	Algeria National PKI Certificate Templates
[FIPS PUB 140-2]	FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
[FIPS 186-4]	FIPS 186-4: Digital Signature Standard (DSS)
[ETSI EN 319 411-2]	ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
[CEN EN 419 221]	CEN EN 419 221: “Protection profiles for TSP Cryptographic modules”
[ISO/IEC 15408]	ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

Table of contents

1 Introduction

The present document is the Certificate Policy (hereinafter, the CP) that applies, and whose compliance is mandated, 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, 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]. Hereinafter, the **TC** and **PSCE** are collectively referred to as the **Trust Services Providers (TSP)**, unless specified otherwise.

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

The CP complies with the formal requirements of Internet Engineering Task Force (IETF) [RFC 3647] with regard to format and content. While certain clause titles are included according to the structure of [RFC 3647], the topic may not necessarily apply in the implementation of the CP. Such clauses are denoted as "*not applicable*".

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

The CP addresses the requirements for the technical, procedural and organizational policies and practices used by the TSPs with regard to all services available during the lifetime of certificates issued by the CA they operate.

The CP is public. It provides a high level of assurance on the identity of the subject of the certificate.

A compliant TSP must have a Certification Practice Statement (CPS) supporting the CP. Where the CP offers options, the CPS must list the choices supported by the TSP's certification services.

A compliant TSP is not required to write its own certificate policy when complying with the CP; it may refer to the CP via its CPS or service policy or terms and conditions. However, compliant TSP may also produce its own certificate policy, based on the CP, by further constraining it. In this case, the TSP's proprietary certificate policy document shall comply with [RFC 3647].

Further information with regard to the CP can be obtained using contact information provided in clause 1.5.

1.1 Overview of the Algerian National PKI management framework

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

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

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

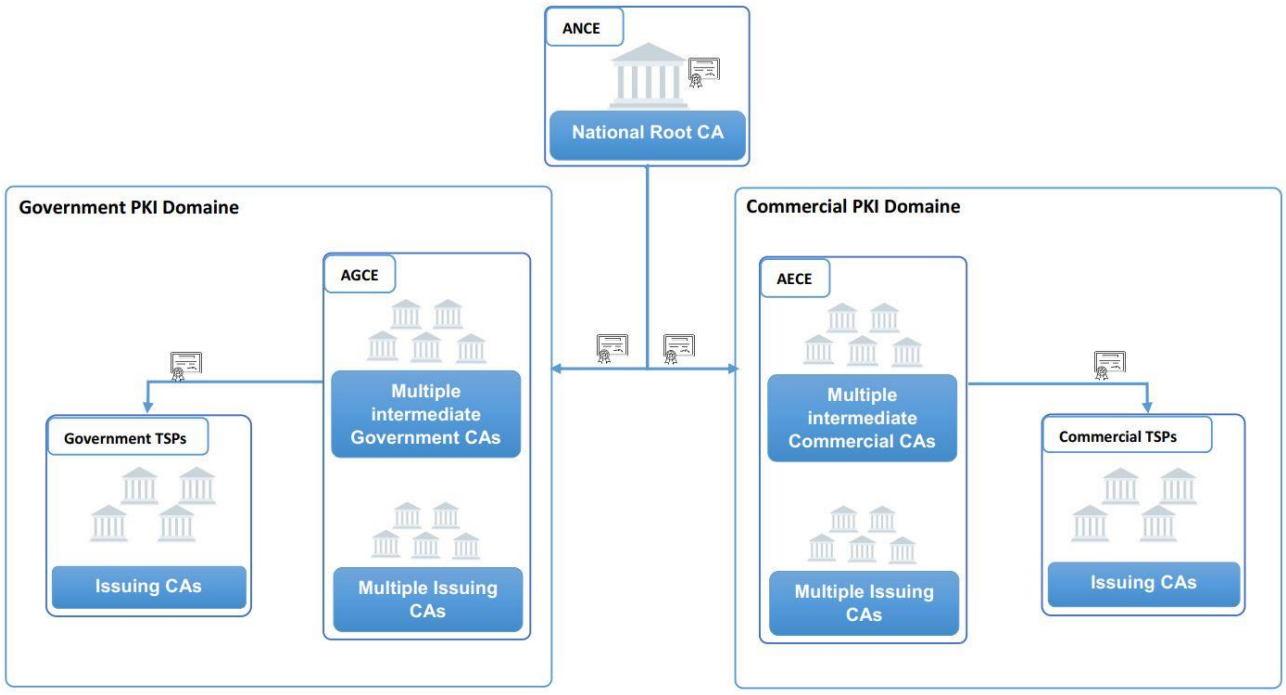

Figure 1: The Algerian National PKI hierarchy

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

- **Government CAs:** Three (03) Intermediate CAs certified by the Root CA, namely: **Government CA, Government TLS CA, and Government TS CA.**

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

  - **Corporate CA:** CA that will issue Digital Signature and Authentication certificates to natural persons (government employees) and legal persons (government entities).
  - **OV TLS CA:** CA that will issue organization validated Server Authentication certificates to non-natural entities such as servers, VPN anddevice certificates. It will also issue Client Authentication certificates to organization's end entities devices.
  - **Trust services CA:** CA that will issue timestamping certificates for AGCE and Government TSPs operating Timestamping services. It will also issue signing certificates to governmental TSPs operating Signature verification services to digitally sign verification responses.

In addition to the above issuing CAs, there is a possibility for a Government entity to operate a TSP by establishing their own certification services under one of the Government CAs. The relevant Government CA will certify one or multiple issuing CAs operated by the Government TSP. This CA shall be technically

constrained where the TSP issuing CA certificate (issued by the Government CA) will be populated with a combination of extended key usage and name constraints 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 Government entity TSP that shall successfully complete an authorization process.

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

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

Commercial CAs:

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

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

In addition,theoverall mandate of the AECE is to authorize and supervise the operations of organizations offering certification and trust services to be certified by the COM-CA.

Commercial TSPs will establish certification services under the COM-CA as following:

The COM-CA will certify one or multiple issuing CAs operated by the TSP. In this case the TSP issuing CA shall be technically-constrained where the TSP issuing CA certificate (issued by the COM-CA) will be populated with a combination of extended key usage and name constraints extensions to limit the scope within which the issuing CA from the TSP may issue end-user certificates.

The AECE is responsible for the supervision and authorization of the TSP that shall successfully complete an authorization process. The details of the supervision and authorization process from the AECE is documented in the "AECE supervision system for TSPs under the commercial domain" document.

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

The certificate policies relating to the issuance of certificates to and by the NR-CA, the Government CA and the Commercial CA are specified in the Certificate Policy and Certification Practice Statement (hereinafter, CP/CPS) of these certification authorities.

The present document applies to the issuance of end-entity certificates by both Government and Commercial TSPs.

1.2 Document Name and Identification

The present document, i.e. the CP, is named " Certificate Policy for TSPs issuing publicly trusted certificates" and will be referenced in related documents through [TSP-CA CP].

The **OID 2.16.12.3.1.2.1** is used to identify the CP:2.16.12(Algeria).3(PKI).1(PMA).2(Policy).1(national TSP-CA CP)

Whenever a TSP operating certification services in accordance with the CP has further constrained the present CP into its own certificate policy, it may also use its own OID in the TSP-CA certificate in addition to the above-mentioned CP OID.

1.3 PKI Participants

Several parties constitute the participants of the TSP-CA PKI, including:

- The NR-CA root signing the Governmental CA and the Commercial CA;
- The upper CA that will "Sign" the TSP-CA, that could be either:
    - The GOV-CA for Government TSPs; Or
    - The COM-CA for Commercial TSPs;
- The TSP-CA, i.e. the certification authority of the TSP;
- Registration Authorities (RA) used by the TSP to enroll end-entities to which end-entity certificates will be issued;
- Subscribers;
- Relying parties.

These participants, collectively called PKI participants, and their roles are described in the following sections.

1.3.1 Certification Authorities

1.3.2 National Root Certification Authority

The NR-CA is under the responsibility of the PMA. The NR-CA is operated by the AGCE, as per the delegation from the PMA to the AGCE. However, the PMA assumes the RA role for the NR-CA. The NR-CA is at the top-level of the national PKI hierarchy.

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

1.3.3 Government Certification Authorities

The AGCE implements and operates multiple intermediate CAs certified by the NR-CA. Each CA is certified to cover a dedicated extended key usage under the Government PKI domain. The overall mandate of the AGCE is to operate a hierarchy of CAs and to offer related trust services to the Algerian government PKI domain. In addition, the AGCE is responsible for authorizing government TSPs offering certification services under the

GovernmentCAs. The Government CAs operates in accordance to the "Government CA CP/CPS" that is identified by the OID 2.16.12.3.2.1.1.

1.3.4 Commercial Certification Authority

The AECE implements and operates multiple intermediate commercial CAs (COM-CAs)certified by the NR-CA. The overall mandate of the AECE is to supervise and authorize the establishment of commercial (non-Government) TSPs offering certification services to be certified by the COM-CA. The COM-CA operates in accordance to the "AECE – Commercial CA CP/CPS" that is identified by the OID 2.16.12.3.3.1.1.

1.3.5 TSP Certification Authority

A TSP-CA is a subordinate issuing CA operated in Algeria, by a TSP established in Algeria, and which is approved for inclusion in the Governmental PKI domain or in the Economic PKI domain. It is certified by one of the subordinate intermediate CAs of the corresponding PKI domain (GOV-CAs/COM-CA), which is in turn root-signed by the NR-CA.

Each TSP-CA is required to be operated in accordance with a Certification Practice Statement (CPS), implementing and complying with the present CP. This CPS must be established by the TSP owning and operating the TSP-CA. It must describe the practices and requirements applicable to the TSP's certification activities operated through the TSP-CA. This CPS is subject to the approval by the PKI Governance Board (PKI GB) of the corresponding intermediate CA (i.e. the PKI GB of the Governmental PKI domain or of the Economic PKI domain).

Approval activities consist of evaluation of the practices, including policies and procedures, specified with regards to the operation of the TSP-CA, including but not limited to:

- The types of end-entity certificates issued by the TSP-CA and the related certificate life-cycle management procedures (e.g. vetting and registration procedures, revocation procedures);
- Processes and controls in place to maintain logical, physical and environmental security;
- Cryptographic systems and products used to generate, store and manage cryptographic keys.

The Government CA or the Commercial CA PKI GB requires application of technical constraints on the TSP issuing CAs to restrict the issuance of digital certificates, through a combination of constraints, e.g. constraints related to the length of certification paths, to the (extended) usage of the keys, to naming convention and inclusion of certificate policy OIDs. Non-Government TSPs may undergo an independent WebTrust audit in addition to complying with the relevant supervisory requirements indorsed by the PMA.

Under the present CP, the main obligations of the TSP with regards to the operation of a conformant TSP-CA are:

- The life-cycle management of issued certificates, including but not limited to all aspects related to application, issuance and revocation;
- The identification and authentication of subscriber information (e.g. during application and revocation phases) in accordance with the applicable certificate profile requirements;
- The publication of issued certificates to a public repository, when the certificate subscriber provides explicit consent;
- The provision and maintenance of certificate validity status information services through publicly available Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) mechanisms;
- To inform, without delays, the corresponding intermediate CA PKI GB:
    - of any significant change to the provision of its certification services;

- of any incident or compromise related to the provision of its certification services;
- of its intention to cease the provision of its certification services.

A conformant TSP-CA may issue one or more types from the following pre-defined certificate types:

- Natural person certificates for advanced electronic signatures [Nat.A.Sig];
- Natural person certificates for qualified electronic signatures [Nat.Q.Sig];
- Natural person certificates for qualified remote electronic signatures [Nat.Q.R.Sig];
- Natural person certificates for authentication [Nat.Auth];
- Natural person certificates for Qualified Authentication and electronic signatures [Nat.Q.Auth.Sig];
- Legal person (or organization) certificates for electronic seal [Leg.Seal];
- Device certificates (Client authentication) for general identification, authentication or session data encryption purposes [Dev];
- TLS certificates for general identification, authentication or session data encryption purposes [TLS] (applicable only for AGCE;
- VPN certificates for general identification, authentication or session data encryption purposes [VPN] (applicable only for AGCE;
- Verification certificates for non-person [Ver], certificate for signing the signature verification response returned from a signature verification service.

Conformant TSP-CAs shall not issue any other type of certificates.

1.3.6 Registration Authorities (RA)

The TSP operating a conformant TSP-CA shall set up or use a RA system that conforms to the present CP. The RA system consists in Registration Authority Officer (RAO), operators, products, systems, and procedures used by the TSP operating a conformant TSP-CA to validate the identity of subscribers requesting the issuance of certificates from the TSP-CA. The TSP may delegate the RA function to the external organizations that may offer this service by law. In this case, the TSP remains fully responsible and accountable for the operations performed by the delegated RA.

In particular, RA are responsible for:

- Authenticating, approving or rejecting certificate application requests;
- Authenticating, approving or rejecting certificate revocation requests;
- Identify certified entities in accordance with naming conventions defined within the present CP, so that each and every entity is uniquely and unambiguously identified;
- Requesting the TSP-CA to produce the certificates for which the corresponding certificate application requests have been approved;
- Requesting the TSP-CA to revoke the certificates for which the revocation requests have been approved;
- Creating and maintaining an audit-log journal that records all significant events related to the RA's operations and fulfilment of the above-mentioned responsibilities;
- Providing selective access to audit-log journal records as specified in the present CP;
- Implementing other operational controls as specified in the present CP;
- Ensuring that the information that it stores and processes is handled in a manner that is consistent both with the policies and procedures defined in this document and with the PMA security's regulations.

The registration is authorized by personal in trusted role, namely RAOs.

1.3.7 Subscribers

Subscribers are those natural, legal persons or devices that are entitled to request issuance of end-entity certificates either for themselves as certificate subject, or on behalf of certificate subjects. Certificate subjects are one of the following end-entities (i.e. not a CA):

- Natural persons;
- Legal Persons or organizations (e.g. companies, administrations, institutions) or parts thereof;
- Devices.

For any certificate, the subscriber shall sign a subscriber agreement, agreeing on the terms and conditions as set forth by the TSP operating the conformant TSP-CA.

TSPs shall detail the applicable types of subscribers in the corresponding CPS of the conformant TSP-CA.

1.3.8 Relying Parties

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

1.4 Certificate Usage

1.4.1 Appropriate certificate usage

Use of certificates issued by conformant TSP-CAs is restricted by using appropriate certificate extensions with regards to key usage and extended key usage, which shall be configured according to the certificate type.

The CPS of conformant TSP-CA shall specify, in accordance with the present CP and in particular its section 7, the appropriate certificate usage that apply to each type of certificate it issues.

Any certificate issued to a CA or an end-entity under the National Algerian PKI has to ultimately comply with the provisions of the present CP.

1.4.2 Prohibited certificate usage

The CPS of conformant TSP-CA shall specify the certificate usage restrictions that apply to each type of certificate it issues. Any usage of the certificate inconsistent with these restrictions, with the appropriate usage or with the contents of the present CP and the applicable CPS of the TSP-CA shall not be authorized.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The PMA has the overall responsibility for producing, amending and publishing this document. The PMA coordinates with the PKI GBs from AGCE and AECE so that proper communications on this CP happens towards TSPs under the Government and Commercial domains.

1.5.2 Contact details

Questions and queries regarding this CP may be addressed to the PMA at the following address:

Autorité Nationale de Certification Electronique – ANCE

Policy Management Authority
Autorité Nationale de Certification Electronique.
Cyber Park Sidi Abdellah, Bt D,
Rahmania, Zeralda,

Alger.
Tel: + 213 (0) 23 202 327
Fax: + 213 (0) 23 202 327
Email: ANCE.Certification.Info@agce.dz

TSPs may raise questions and queries on this CP to the PKI GB of their respective domain. Contact information to be retrieved from ANCE.

1.5.3 Person Determining CPS Suitability for the Policy

The TSP is responsible for ensuring that its CPS conforms to the present CP.

The competent PKI GB (from AGCE or AECE) is responsible for assessing the actual CPS suitability for the present CP. This process may be supported by a Conformity Assessment Report (CAR) from an auditor as supported in the Algeria National PKI TSP supervision scheme. The ultimate responsible for this suitability is the PMA that takes its final decision upon information provided by the PKI GB (from AGCE or AECE).

1.5.4 CP Approval Procedures

A dedicated process involves the PMA reviewing the initial version of the CP and any subsequent updates. Amendments shall either be in the form of a document containing an amended form of the CP or an update notice.

The PMA communicates with the PKI GBs (from AGCE and AECE) in relation to amendments to this CP and formally approves the newer versions.

1.6 Definitions and Acronyms

1.6.1 Terminology and definitions

The following sections contain the definitions of terms and acronyms used in this CP. The source of a definition is cited when available.

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

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

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.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

CAA: From RFC 6844 (http://tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue."

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.

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.

DNS CAA Email Contact: The email address defined in section A.1.1 of the CA/B Forum Baseline Requirements.

DNS CAA Phone Contact: The phone number defined in Appendix A.1.2 of the CA/B Forum Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Appendix A.2.1 of the CA/B Forum Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Appendix A.2.2 of the CA/B Forum Baseline Requirements.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

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

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

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.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

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

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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.

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.

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.

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.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

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.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

1.6.2 Abbreviations

AATL	Adobe Approved Trust List
AECE	Autorité Économique de Certification Électronique
AGCE	Autorité Gouvernementale de Certification Électronique
ANCE	Autorité Nationale de Certification Électronique
CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CCTV	Closed Circuit TV
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CMC	Certificate Management over CMS
DN	Distinguished Name
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
http	Hyper Text Transfer Protocol
HSM	Hardware Security Module
HVAC	Heating, Ventilation and Air Conditioning
IEC	International Electro-Technical Commission
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security
ISO	International Standards Organisation
ITU	International Telecommunications Union
KGC	Key Generation Ceremony
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier

OCSP	Online Certificate Status Protocol
PKCS # 1	Public Key Cryptography Standards (PKCS) #1
PKCS # 7	Cryptographic Message Syntax
PKCS #10	Certification Request Syntax Specification
PKCS #12	Personal Information Exchange Syntax published by RSA Security
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PKI GB	Public Key Infrastructure Management Board
PMA	Policy Management Authority
PSCE	Prestataire de Service de Confiance Électronique
RA	Registration Authority
RSA	RSA algorithm (from the acronym for the inventors: Rivest, Shamir and Adleman)
SCDev	Signature Creation Device
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TC	Tiers de Confiance
TL	Trusted List
TLS	Transport Layer Security
TS	Trust Service
TSP	Trust Service Provider
TSP/TSTrust Service Provider and the Trust Service(s) it provides	
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier
NTP	Network Time Protocol

2 Publication and Repository Responsibilities

2.1 Repositories

The TSP shall publish and maintain the applicable TSP-CA CPS(s), the relevant policies and agreements (e.g. subscriber, RA and relying party agreements), the TSP-CA(s) certificates, TSP-CA CRLs and other applicable status information and any other related public documents it issues via an online and publicly accessible website (hereinafter the TSP-CA public repository).

2.2 Publication of Certificate Information

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

The TSP shall publish its TSP-CA certificates on its TSP-CA public repository.

The TSP may publish end-entity certificates via its TSP-CA public repository provided it obtained the subscriber's agreement allowing for such publication.

The TSP shall publish certificate validity status information upon regular intervals as indicated in its CPS and in accordance with the present CP. The certificate validity status information service shall be twenty-four by seven service.

2.3 Time or Frequency of Publication Repositories

2.3.1 Certificates

TSP-CA and OCSP certificates shall be published to TSP-CA public repository once they are issued.

2.3.2 CRLs

The TSP shall publish CRLs at regular intervals and include a pointer (URL) to the relevant CRL distribution point into end-entity certificates as part of the CDP extension whenever this extension is present.

The TSP shall maintain its TSP-CA public repository, the CRL distribution point and the information on this URL for a minimum of seven years after the expiration of the last issued certificate including the CRL distribution point.

Versions of TSP-CA related documents approved to be published on the TSP-CA public repository shall be uploaded within seven days maximum.

The following rules shall apply for the CRL issued by the TSP-CAs:

- MUST update and publish a new CRL at least every:

  - seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer"); or

  - four (4) days in all other cases;.

- MUST update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked

2.4 Access Controls on Repositories

TSP-CA CPS, certificates and CRLs and any other data published to the TSP repository shall be available with unrestricted read access.

Access control mechanisms shall be implemented on the repositories operated by TSPs to preserve the repositories availability and prevent any unauthorized addition or modification of any published data.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of names

The certificates issued by the TSP-CAs shall contain X.500 Distinguished Names (DNs). The DN formats allowed are:

For Certificates issued to Natural persons:

- givenName=<(optional) as on government-issued ID card>;
- surName=<(optional) as on government-issued ID card>;
- SERIALNUMBER = <unique identifier for each individual as constructed by the RA>;
- cn= <concatenation of given name and surname as in government-issued ID 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) the province that the person belongs to>;
- 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.

Device authentication certificates:

- subjectAltName = <System unique common name, unique device identifier or IP address that are applicable>
- cn= <System unique common name, unique device identifier or IP address that are applicable>,

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 device operates>,
- c = DZ

VPN certificates:

- subjectAltName = <System unique common name, unique device identifier or IP address that are applicable>
- cn= <System unique common name, unique device identifier or IP address that are applicable>,
- 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 device operates>,
- c = DZ

TLS/SSL certificates:

- subjectAltName = <public IP or FQDNs or authenticated domains that are under the control of the Subscriber >
- cn = <FQDN(s) or public IP address, potentially linked to the subjectAltName>
- 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 device operates>,
- c = DZ

OCSP:

- cn= <friendly name of the OCSP service from the TSP-CA>,
- o = <full registered name of organization to which the certificate is issued>,
- s = the province where the OCSP operates,
- c = DZ

3.1.2 Need for Names to be Meaningful

All end-entity certificates issued by the TSP-CA shall be meaningful and shall uniquely identify the subject.

3.1.3 Anonymity and Pseudonymity of Subscribers

This CP does not permit anonymous or pseudonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in certificates issued by TSP-CAs are interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

The TSP shall enforce the controls that are necessary to guarantee that subject Distinguished Names (DN) are unique. Minimum controls enforced:

- For certificates issued to natural and legal persons, the TSP shall enforce a convention for a meaningful representation uniquely identifying the individual.
- Certificates issued to devices shall uniquely identify the device. Options include using the registered public DNS name or public IP addresses.

3.1.6 Recognition, authentication and role of Trademarks

TSP certificate applicants are prohibited from using names in their certificate requests that infringe intellectual property rights of others. Certificate applicants shall provide reasonable evidence that the used names/trademarks belong to them.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The RA shall enforce submission of a proof of possession of the private key as part of certificate requests (e.g., PKCS#10, CMC).

3.2.2 Authentication of Organization Identity

For organizations requesting certificates from a TSP, the identity and related information of the organization shall be validated by the corresponding TSP RA through a reliable authoritative source that allows the verification of the organization's legal name and legal representatives (e.g. the Algerian Official Journal (Journal Officiel) for Government entities, and the Chamber of commerce or Trade Register for the Commercial domain). The below table elaborates further on the validation requirements:

Certificate type	Identity validation requirements
• Legal person (or organisation) certificates for electronic seal	**Legitimacy** TSPs shall perform the following validations for the entity to which the certificate is requested: • Verify the existence of the entity using an authoritative source that is expected to provide detailed information about the entity including its legal name, address, trade name (if applicable) and the entity's authorized representatives. • Verify the authority of entity authorized representative requesting the certificate. The requestor shall be an authorized representative from the entity (as referenced in the entity's record at the authoritative source). **Binding** The organization name to be inserted in the requested certificate must exactly match the legal name of the Government entity requesting the certificate unless there is an authentic proof linking the entity with the name to be included in the certificate. The identity of the Government entity representative (certificate requester) shall be validates as specified for the qualified signing above.
• Certificates issued by AGCE (Device certificates, SSL/TLS certificates, VPN certificates and Verification certificates)	**Legitimacy** TSPs shall: • Verify the existence of the Entity using an authoritative source; • Verifies the authority of entity authorized representative requesting the certificate. The requestor shall be an authorized representative from the entity (as referenced in the entity's record at the authoritative source in use). **Binding** TSPs shall: • Validate the association between the certificate requester (applicant) and the entity to which he/she belongs;

	• Validate the system/device/domain control/ownership.

3.2.3 Authentication of Individual Identity

3.2.3.1.1 Tools and mechanisms for Authentication of Individual Identity

This section defines tools and types mechanisms that can be used for identification and authentication of an individual's identity.

3.2.3.1.2 Types of evidences:

Primary Evidences:

Primary evidences are defined as governmental authoritative sources including secure photo ID evidence, issued with robust identity proofing, issuance and management processes. Examples of Primary evidences are: passports, (electronic) citizen identity cards, (electronic) resident identity cards, (international) driving license, civil servant cards, police forces identification cards.

Secondary Evidences:

Secondary evidences are government authoritative sources that are supported by moderate identity proofing, issuance and management processes. Examples of Secondary evidences are: professional corporation card (e.g. Bar association, Healthcare professional association), population register excerpts, tax register excerpts, social security register excerpts.

3.2.3.1.3 Authoritative source

An authoritative source is any source, irrespective of its form, that is nationally trusted to provide valid and accurate data, information and/or evidence that can be used to prove the identity of an individual. A source may only be authoritative for the data provided by it.

It is important to ensure that an information claimed to be provided by a claimed authoritative source is authentic, i.e. that it originates from a known authoritative source, is genuine and its integrity has been verified.

Examples of authoritative sources can include:

- National Population registers for information on person's identity data;
- Government registers which have associated governing processes to ensure reliable and correct data such as passport registers, driving license databases, tax registers, social security registers;
- Official identity documents such as passports and identity cards.

3.2.3.1.4 Identity validation requirements

Certificate type	Identity validation requirements
• Natural person certificates for advanced electronic signatures • Natural person certificates for authentication	**Legitimacy** TSPs shall: • Verify that the applicant's email address exists, and that the subscriber has control over an existing email address (i.e. ownership and control of email)

•	• Primary or Secondary pieces of evidence of the following
	  o Applicant's full name, and date and place of birth,
	  o Linkage between the identity of the Subject of the certificate and a legal person (organization, corporation) identity when the subject is a natural person who is identified in association with a legal person
	• TSPs shall validate the authenticity of submitted evidences to establish that:
	- They are valid pieces of evidence: Checking should rely on national guidance on how to verify the authenticity and security features of national official identity documents. With regards to foreign identity documents, checking may rely on the guidance provide on PRADO (Public Register of Authentic travel and identity Documents Online)1 or any similar database or guidance on how to verify some of the most important security features of official documents issued around the world.
	- The identity is not that of a deceased person (individual) or of a terminated person (organization/corporation).
	
	Binding
	TSPs shall verify the link between the claimed identity and the claimant through the following mechanisms:
	• By an RA office through authentication credentials exchanged with the claimant using his verified email address and/or a mechanism that involves live video session with the claimant that involves the presentation of a "Primary evidence" or "Secondary evidence" used earlier.
	• Existing authentication credentials from accepted Identity Providers in Algeria provided that the following requirements are met:
	- Existence of ID proofing artifacts substantiate the antecedent verification outcome
	- Mechanisms are in place that bind the individual to the asserted identity

• Natural person certificates for qualified electronic signatures • Natural person certificates for Qualified Remote electronic signatures	**Legitimacy** TSPs shall: • Verify that the applicant's email address exists, and that the subscriber has control over an existing email address (i.e. ownership and control of email) • Primary and Secondary pieces of evidence of the following o Applicant's full name, and date and place of birth,

[1] https://www.consilium.europa.eu/prado

	○ Linkage between the identity of the Subject of the certificate and a legal person (organization, corporation) identity when the subject is a natural person who is identified in association with a legal person • The applicant shall provide all evidences at an in-person interview or through an equivalent method. • Validate the authenticity of submitted evidences to establish that: - They are valid pieces of evidence: Checking should rely on national guidance on how to verify the authenticity and security features of national official identity documents. With regards to foreign identity documents, checking may rely on the guidance provide on PRADO (Public Register of Authentic travel and identity Documents Online)2 or any similar database or guidance on how to verify some of the most important security features of official documents issued around the world. - The identity is not that of a deceased person (individual) or of a terminated person (organization/corporation). **Binding** TSPs shall verify the link between the claimed identity and the claimant as part of a physical in-person interview or equivalent via one of following methods: - Visual face-matching by an RA office through a video session with the claimant that involves the presentation of a "Primary evidence"; - Biometric verification involving face matching and liceness against international published identity proofing standards related to.

3.2.4 Authentication of Domain name

For SSL/TLS certificates, the control or ownership of the domain name(s) which is/are specified in the certificate application shall be verified..

3.2.5 Non-verified subscriber information

Every subscriber information contained within certificate issued by the TSP-CA shall be verified by the corresponding TSP RA.

3.2.6 Validation of Authority

Refer to section 3.2.2 and 4.2.

3.2.7 Criteria for Interoperation

No stipulation.

[2] https://www.consilium.europa.eu/prado

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Keying

Identification and authentication steps for Routine Re-Key shall be the same as applied during initial certification.

3.3.2 Identification and Authentication for Re-Key after revocation

Identification and authentication procedures for re-key after revocation shall be the same as during initial certification.

3.4 Identification and Authentication for Revocation Requests

The TSP RA shall enforce identification and authentication for revocation requests.

The TSP RA shall validate the revocation request and the identity of the revocation request applicant.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate application for TSP-CA under one of the GOV-CAs shall be limited to subscribers being part of or formally related to the Algerian Government and shall be limited to the certificate types defined in section 1.4.1. The subscriber community for such TSP shall be limited to the TSP's employees (and contractors) or to a user base that the TSP is authorize to service by law

Certificate application for TSP-CA (PSCEs) under the COM-CA shall be limited to the certificate types defined in section 1.4.1. The subscriber community for such TSP shall be limited to a user base that the TSP is authorize to service by law

4.1.2 Further details and restrictions shall be specified in the applicable TSP CPS.Enrolment Process and Responsibilities

For any requested certificate, the subscriber shall ratify a dedicated subscriber agreement.

Further details on the enrolment process shall be specified in the applicable TSP CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Refer to section 3.2 of this CP.

In addition, the following vetting procedure requirements apply:

a) Vetting procedures are required as part of the certificate request processes performed by the TSP with regards to the TSP-CA;
b) Actual procedures used by the TSP with regards to the TSP-CA shall be documented in the applicable TSP CPS;
c) 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) shall be stored along with the application record;

c. Any malicious certificate or revocation request or a request that fails multiple (more than 5) times shall be added to a blacklist.
d. The blacklist shall be designated per type of certificate and include the necessary details of the requestor to successfully and unambiguously identify future malicious requests.

d) specific requirements based on the type of applicant/certificate:
   a. For end-entity natural person certificates issued by a TSP-CA within the Governmental PKI domain:
      i. Sign the subscriber agreement;
      ii. Blacklist check according to the RA's own blacklist;
      iii. If the applicant is in the blacklist, the verification procedure is rejected then further conversation is held with the entity's official representative. In case of positive outcome, the vetting procedure continues;
      iv. Identify the individual (as described in section 3.2.2) and confirm his association with the government entity he/she belongs to according the entity internal (human resource) processes.
   b. For electronic seal certificates issued by a TSP-CA within the Governmental PKI domain
      i. Sign subscriber agreement;
      ii. Blacklist check:
         1. Using the local blacklist;
         2. If the requestor/organization is in the blacklist, the verification procedure is rejected. In case of positive outcome, the vetting procedure continues;
      iii. Establish government entity existence:
         1. The Government entity requesting a certificate and the organization name to be inserted in the requested certificate must match the formally registered name of the Government entity exactly unless there is an authentic proof lining the entity with the name included in the certificate. The full name or the abbreviated version may be added to the certificate.
         2. The Government Entity existence may be verified using an authoritative source of Government Entities which is expected to contain detailed information about the entity including its formal name and authorized representatives.
         3. 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;
      iv. Establish government entity authorized representatives: The requestor must be an authorized representative from the Government entity (as referenced in the entity's record in the authoritative source or an individual previously dully authorized/delegated by a verified authorized representative). This authorization shall be embedded in the request form;
      v. Identify authorized certificate requestors of government entity.
   c. For SSL/TSL certificates issued by a TSP-CA within the Governmental PKI domain:
      i. Sign subscriber agreement;
      ii. Blacklist check (see above);
      iii. Establish government entity existence & authorized representatives (see above);
      iv. Identify authorized certificate requestors of government entity;
      v. In case of having the wildcard character (*) in the CN or subjectAltName, the following validations apply:
         1. Wildcard SSL Certificates include a wildcard asterisk character as the first character in the Common Name (CN) attribute of the Subject field and or in the SubjectAltName extension.

2. The wildcard asterisk character must not fall within the label immediately to the left of a registry-controlled or public suffix.
3. Certificate issuance is rejected unless the applicant proves its rightful control of the entire Domain Namespace.

vi. Check for valid domain TLD;
vii. Check for high-profile certificate requests;
viii. Check CAA records for the domain;
ix. Verify ownership of the domain name:
    1. Perform e-mail validation consisting of sending an e-mail with a random, unique value to an administrative e-mail address associated with the domain (i.e. admin@example.com). This validation may be performed using following e-mail addresses: admin@, administrator@, webmaster@, etc. The admin must reply with the random value within 3 days maximum. Consider other alternate methods and eventually cancel request and add to black list.
    2. Perform Web site control check by requesting a change to the website, e.g. requesting to upload a file with a unique random value. This verification must be conducted within 03 days maximum. Offer the certificate requestor to perform one of the other SSL Domain control validation steps or finally cancel the certificate request.
    3. Perform DNS validation by requesting to proof ownership over a domain by performing changes to the DNS configuration of the domain. Specifically, request the certificate requestor to add/change the CNAME, TXT and CAA record to contain a unique random value. The DNS record can be checked using dedicated commands. This DNS validation procedure must be executed within 3 days.

    In case if an IP(s) is added in the certificate, the below ownership validations shall be followed instead:

    1. Proof control over the IP Address by asking the application to apply an agreed-upon change to information found on an online Web page identified by a URI containing the IP Address;
    2. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name;
    3. Requesting documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry;
    4. Email challenge based on email address or via phone information listed in the IANA or similar repository.

d. For VPN certificates issued by a TSP-CA within the Governmental PKI domain:
    i. Sign subscriber agreement;
    ii. Blacklist check (see above);
    iii. Establish government entity existence & authorized representatives (see above);
    iv. Identify authorized certificate requestors of government entity;
    v. Verify the device eligibility for certification and the device control by certificate requester:
        1. The RA identifies the IT system or device for which certificate(s) shall be requested from the TSP-CA. These IT systems or devices must be part of the IT infrastructure of a government entity.
        2. The RA verifies that the applicant is a legitimate sponsor or authorized device or system administrator of the device or system for which certificate(s) shall be requested.

Similar vetting procedures are required for certificates issued by TSP-CA operated by TSPs within the Commercial PKI domain with the following exceptions:

a) Entity existence shall be verifying through an authoritative source such as Chamber of Commerce or Trade Register. Such mechanisms shall be agreed and approved by the COM-CA PKI GB;
b) The association between the applicant and the entity it belongs to shall be verified according to procedures approved by the COM-CA PKI GB.

4.2.2 Approval or Rejection of Certificate Applications

The TSP RA shall accept the certificate application and request a digital certificate to the CA only when all verifications undertaken by the RA are successful, amongst others:

- Subject and subscriber identity verification;
- Proof of possession of private key;
- Proof of ownership of the device, when applicable;
- Proof of association with an organization;
- Any other conditions or constraints such as defined in the CPS, in particular with regard to who can request a certificate.

The TSP CPS shall describe further applicable specification details.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

The TSP-CA shall process a certificate issuance request as follows:

- Verify that the certificate request originates from a valid RA;
- Issue the required digital certificate containing the information provided in the certificate request and the applicable certificate policy OID(s):
- When applicable, publish the issued certificates on the TSP-CA public repository.

When the issuance of the certificate is delayed from the registration process, the TSP-CA may only issue the certificate if the information and supporting evidences checked during this registration process are still valid.

The TSP CPS shall describe further applicable specification details.

4.3.1 CA Actions during Certificate Issuance

The TSP CPS shall describe further applicable specification details.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The TSP CPS shall describe further applicable specification details.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

It shall be possible for the subscriber to verify that the issued certificate contains the required data.

The certificate acceptance shall be clearly explained to the subscriber and accepted through the ratification of the subscriber’s agreement.

The TSP CPS shall describe further applicable specification details.

4.4.2 Publication of the Certificate by the CA

The TSP-CA may publish the issued certificates on the TSP-CA public repository as specified in section 2.2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber duties

When using a subscriber's private key and the corresponding certificate, a subscriber shall adhere to the following obligations:

- Use the private key and corresponding certificate only for their intended usage as per the present CP and the applicable TSP CPS;
- Discontinue using a private key following expiration or revocation of the corresponding certificate;
- Notify the RA, without any delay, in the event of private key compromise.

4.5.2 Relying party duties

When using a subscriber's public key and the corresponding certificate, a relying party shall adhere to the following obligations:

- Ensure that
    - the public key is appropriate for the intended use as set forth in the present CP and the applicable TSP 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;
- Check the validity status of the certificate through the OCSP service offered by the TSP-CA and current CRLs.

4.6 Certificate Renewal

Certificate Renewal shall not be supported.

4.7 Certificate Re-key

Certificate re-key is an operation supported by the provisions of the present CP. The re-key process (including identity validation, issuance) shall be similar to the initial certification.

The TSP may re-use evidences provided during the registration process only if these evidences are still valid at the time of re-key.

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 should invalidate any existing active certificates of the same type.

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

The present CP does not specify provisions for certificate modification outside the context of certificate re-key, which results in the generation of a new certificate with the same identification information. Refer to section 4.7 for further details.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The TSP-CA shall revoke an issued certificate under the following circumstances:

- Upon request from the subscriber or a representative
- Knowing that the information on the certificate is no longer accurate
- Discovering that the certificate was issued in a manner not materially in accordance with the procedures required by this CP / the applicable TSP CPS
- Determination that the certificate was issued to a subject other than the one named as the subject of the certificate
- The subscriber has been declared legally incompetent
- Obtaining an evidence that the certificate was misused
- Obtaining or discovering evidence that subscriber’s private key, corresponding to the public key certificate, has been compromised or that there is a demonstrated or proven method that exposes the subscriber's private key to compromise
- Receiving a lawful order from a law enforcement organization in Algeria to revoke a certificate
- The subscriber has been declared legally incompetent

The present CP does not specify provisions for revoking an OCSP certificate or digital certificates corresponding to the TSP-CA organization apart from the compromise of the related key pair, which shall be

considered by the TSP as a TSP-CA disaster and treated as such in conformance with its disaster recovery and business continuity procedures.

The TSP applicable CPS shall specify any additional relevant revocation circumstances in full compliance with the applicable baseline requirements provisions.

The following sub-sections focus only on the revocation provisions that apply to end-entity certificates issued by the TSP-CA.

4.9.2 Who Can Request Revocation

The subscriber shall be able to request the revocation of his certificate.

The TSP-RA shall be allowed to revoke subscriber certificates.

Only authorized revocation requests shall be accepted.

The TSP CPS shall describe further applicable specification details.

4.9.3 Procedure for Revocation Request

The TSP CPS shall describe further applicable specification details.

4.9.4 Revocation Request Grace Period

There shall be no revocation grace period.

Revocation requests shall be processed as per schedule or immediately by the TSP RA.

4.9.5 Revocation Request Response Time

Certification revocation requests and problem reports shall be processed within 24 hours from their reception.

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 or through its OCSP responder.

Relying parties shall use any of these methods while processing a certificate issued by a TSP-CA.

4.9.7 CRL Issuance Frequency

CRLs shall be issued as per section 2.3 of the present CP.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 Online Revocation/Status Checking Availability

OCSP responder(s) shall conform to RFC 6960.

OCSP information shall be available immediately to relying party applications.

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

4.9.10 Online Revocation Checking Requirements

It is at the discretion of the relying party to decide whether to use CRL or to rely on OCSP based on their PKI application constraints and business needs.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements — Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Certificate suspension shall not be supported by the TSP-CA.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.10 Status Services

Refer to section 4.9.6.

4.10.1 Operational Characteristics

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

The OCSP responders shall expose an HTTP interface accessible to relying parties.

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The TSP CPS shall describe the conditions for ending the subscriptions from the TSP subscribers.

4.12 Key Escrow and Recovery

Key escrow shall not be supported by the TSP-CA.

5 Management, Operational and Physical Controls

The below minimum controls shall be enforced by TSPs compliant to this CP.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

All critical components of the PKI solution shall be housed within a highly secure enclave within the TSP facilities.

Physical access controls shall be in place to protect the infrastructure, management systems and related operational activities of the PKI solution.

5.1.2 Physical Access

Physical security controls shall include security guard-controlled building access, man-traps, biometric (e.g. IRIS access) and Closed-Circuit TV (CCTV) monitoring. These physicals controls must protect the hardware and software from unauthorized access and shall be monitored on a 24x7x365 basis.

5.1.3 Power and Air Conditioning

The secure enclave shall be furnished with a UPS, and heating ventilating and air conditioning (HVAC) sufficient to maintain the computer equipment within the manufacturers' recommended range of operating temperatures and humidity.

5.1.4 Water Exposures

The PKI shall be installed in such a way that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

The enclave shall be protected from fire and heat by smoke detection equipment that is monitored on a 24x7x365 basis.

Fire suppression equipment shall be installed within the enclave.

5.1.6 Media Storage

Electronic optical and other media shall be stored so that they are protected from accidental damage (water, fire, electromagnetic radiation).

Media that contains audit archives and backup information shall be stored in a secure fire-proof safe while it is stored within the enclave.

5.1.7 Waste Disposal

All obsolete paper, magnetic media, optical media created within the enclave shall be shredded before discarding.

Reusable magnetic and optical media may be reused indefinitely within the enclave, but must be properly wiped and/or destroyed depending on the confidentiality of the data stored on the medium.

5.1.8 Offsite Backup

System backups must provide sufficient recovery information to allow the recovery from system failure(s).

Backups shall be made on a daily basis and copies shall be transferred to a secure offsite location on a periodic basis.

Backup media shall be stored in a location separate from the TSP-CA main site.

Facilities used for offsite backup and archives shall have the same level of security as the TSP-CA main site.

5.2 Procedural Controls

The TSP-CA shall follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

The TSP-CA shall obtain a signed statement from each member of the staff concerned on not having conflicting interests with the CA activities, maintaining confidentiality and protecting personal data.

5.2.1 Trusted Roles

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives).

The TSP-CA shall conduct an initial investigation of all members of staff who are candidates to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

5.2.2 Number of Persons Required Per Task

The TSP-CA shall maintain and enforce rigorous control procedures to ensure the segregation of duties, based on job responsibility, in order to prevent single trusted personnel to perform sensitive operations.

The most sensitive tasks, such as access to and management of CA cryptographic hardware security module (HSM) shall require the involvement of two or more persons.

5.2.3 Identification and Authentication for Each Role

Before exercising the responsibilities of a trusted role:

- The TSP-CA shall confirm the identity of the employee by carrying out background checks.
- The TSP-CA shall issue an access card to administrators who need to access equipment located in the secure enclave.
- The TSP-CA shall provide the necessary credentials that allow administrators to conduct their functions.

5.2.4 Roles Requiring Separation of Duties

The TSP-CA shall ensure separation among the following discreet work groups:

- Personnel managing operations on certificates
- Administrative personnel who operate the supporting platform
- Security personnel who enforce security measures
- Audit personnel who review the audit logs

5.3 Personnel Security Controls

The TSP shall ensure implementation of security controls with regard to the duties and performance of the members of its staff with regards to the TSP-CA activities.

These security controls shall be documented in an internal confidential policy and include the areas below.

5.3.1 Qualifications, Experience, Clearances

The TSP shall ensure that checks on the members of its staff are performed to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks include:

- Criminal convictions for serious crimes;
- Misrepresentations by the candidate;
- Appropriateness of references; and
- Any clearance as deemed appropriate.

5.3.2 Background Checks and Clearance Procedures

The TSP shall make the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

5.3.3 Training Requirements and Procedures

The TSP shall make available relevant technical training to their personnel in order for them to perform their functions.

For personnel performing information verification duties (i.e. RA officers), public key infrastructure topics, authentication, vetting policies and procedures, applicable certificate policy and CPS material as well as common threats to the information verification process shall be included in the training.

The required skills and knowledge for validation specialists shall be tested through an examination on the information verification requirements.

5.3.4 Retraining Period and Retraining Procedures

Periodic training updates shall be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions against Personnel

The TSP shall sanction personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the TSP-CA personnel, as it might be appropriate under the circumstances and as per the prevailing HR Policy and Country Law.

5.3.7 Independent Contractors Requirements

TSP-CA independent subcontractors and their personnel are subject to the same background checks as the TSP personnel with regards to the TSP-CA activities. The background checks shall include:

- Criminal convictions for serious crimes;
- Misrepresentations by the candidate;
- Appropriateness of references;
- Any clearance as deemed appropriate;
- Privacy protection; and
- Confidentiality conditions.

5.3.8 Documentation Supplied to Personnel

The TSP shall make available documentation to personnel describing their duties and the operational processes they are fulfilling.

5.4 Audit Logging Procedures

Details on the audit logging procedures shall be defined in the applicable CPS.

The present CP specifies requirements on audit logging procedures as per the following sections.

5.4.1 Types of Event Recorded

The following events occurring with regards to the TSP-CA shall be recorded:

- TSP-CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, and destruction;
  - Cryptographic device life cycle management events;
- TSP-CA and Subscriber Certificate life cycle management events, including:
  - Certificate requests, re-key requests, and revocation;
  - All verification activities stipulated in these requirements and the TSP-CA's CPS;
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
  - Acceptance and rejection of certificate requests;
  - Issuance of certificates;
  - Generation of CRLs and OCSP responses;
- Security events, including:
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes system crashes, hardware failures and other anomalies;
  - Firewall and router activities;
  - Entries to and exits from the CA facility.

The TSP may maintain additional audit trails of relevant TSP-CA operational as deemed necessary for continuance compliance to the Baseline Requirements.

5.4.2 Frequency of Processing Log

The TSP shall ensure that the designated personnel reviews log files at regular intervals in order to validate log integrity and ensure timely identification of anomalous events.

Designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity.

Log files and audit trails shall be periodically archived for inspection by authorized personnel and designated auditors.

The log files shall be properly protected by an access control mechanism, so that no others can have access. Log files and audit trails shall be backed up.

All log entries include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry;
- Description of the entry.

5.4.3 Retention Period for Audit Log

The audit log files shall be retained as per the retention period stated in the Baseline Requirements.

5.4.4 Protection of Audit Log

Audit logs shall be protected by a combination of physical, procedural and technical security controls.

5.4.5 Audit Log Backup Procedures

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

- Backup media shall be stored locally in the TSP-CA main site in a secure location.
- A second copy of the audit log data and files shall be stored outside TSP-CA main site, in a site that provides similar physical and environmental security as the main site.

5.4.6 Audit Collection System (internal vs. external)

No Stipulation.

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

TSPs shall perform annual risk assessments on their CA systems to cover the following scope:

- The identification of potential internal and external threats that could result in the compromise of the CA systems and assets
- The assessment of the likelihood and potential damages of the identified threats
- The establishment of the residual risks considering the implemented controls in place
- The definition of new arrangements/controls as applicable to mitigate the residual risks
- The agreement with the TSP top management on a plan to implement the new arrangements/controls

TSPs shall also plan and perform regular vulnerability assessment (at least quarterly) and penetration testing (at least once a year) on CA systems as per the Baseline Requirements.

5.5 Records Archival

5.5.1 Types of records

The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof.

5.5.2 Retention period

Archived records shall be retained as per the requirements of the Baseline Requirements.

5.5.3 Protection of archive

The TSP shall archive audit logging data on a regular basis and keep archived data in a retrievable format.

The TSP shall ensure the integrity of the physical storage media and implement proper backups to prevent data loss.

The TSP shall ensure that records are archived in such a way that they cannot be deleted or destroyed. Controls shall be in place to ensure that only authorized personnel are able to manage the archive without modifying integrity, authenticity and confidentiality of the contained records.

5.5.4 Archive backup procedures

The TSP CPS or related documentation shall provide details on how archive records are backed up.

5.5.5 Time-stamping of records

All recorded events by the TSP-CA shall include the date and time of when the event took place, based on the time of the operating system.

The TSP CPS shall document further details including the controls in place to ensure that all TSP-CA systems rely on and are synchronized with a trusted time source.

5.5.6 Archive Collection

Only authorized and authenticated personnel shall be allowed to handle archived material.

5.5.7 Procedures to obtain and verify archive information

Only TSP staff members with a clear hierarchical control and a definite job description may obtain and verify archived information. The TSP shall retain records in electronic or paper-based format.

5.6 Key Changeover

The TSP may periodically changeover its TSP-CA keys. Private keys may be maintained until such time as all relying certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

In a separate internal document, the TSP shall specify applicable incident, compromise reporting and handling procedures.

The TSP shall specify the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

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

The TSP and all other PKI Participants (other than Subscribers and Relying Parties) shall establish the necessary measures to ensure full recovery of the TSP-CA services in case of a disaster, and corrupted servers, software or data.

The TSP shall establish:

- Disaster recovery resources in a location sufficiently distant from the regular TSP-CA operation facility;
- Fast communications between the two sites
- Disaster recovery infrastructure and procedures shall be fully tested at least once a year.

5.7.3 Entity private key compromise procedures

For Subscribers key compromise, see section 4.9 of the present CP.

In the event of a key compromise of a TSP-CA, the following actions shall be taken by the TSP:

- The corresponding intermediate CA PKI GB shall be notified as soon as there is an indication of suspected compromise. The TSP shall work together with that intermediate CA PKI GB on deciding whether to continue TSP-CA activities or cease operations.
- All active certificates issued by the TSP-CA shall be revoked.
- Organizations holding end-entity certificates shall be notified.
- A TSP-CA compromise notice shall be published toward relevant relying parties.

5.7.4 Business continuity capabilities after a disaster

The TSP shall establish the necessary measures for full and automatic recovery of the on-line services, such as CRL distribution and OCSP services, in case of a disaster, corrupted servers, software or data.

The TSP shall establish the necessary measures to ensure full recovery of the off-line services service in case of a disaster, corrupted servers, software or data.

These measures shall be described in a Business Continuity Plan (BCP) available as a separate internal document, to be implemented to ensure business continuity following a natural or other disaster.

The business continuity plan shall include the following:

1. Conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. Maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. The plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e. secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time;
13. How frequently backup copies of essential business information and software are generated;
14. The distance of recovery facilities to the main site;
15. 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.

5.8 CA or RA Termination

If the TSP and/or the corresponding intermediate CA PKI GB determine that termination of the TSP-CA services is deemed necessary, the TSP shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

Procedures shall exist for informing affected entities and for transferring archived TSP-CA records to an appropriate custodian.

The TSP shall arrange for the retention of archived data specified in section 5.5 of the present CP, taking into account the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate.

Before termination of the TSP-CA activities, the TSP shall:

a. Provide a written notice to the corresponding intermediate CA PKI GB of its intention to cease operating its TSP-CA activities, together with a copy of the TSP's termination plan, at least ninety (90) days before:
    i. the date when it will cease to the TSP-CA related activities;
    ii. expiry, when applicable, of the TSP authorization for providing its TSP-CA activities, where the TSP has no intention to apply for an authorization renewal.
b. Provide a written notice to its subscribers of its intention to terminate its TSP-CA activities within at least sixty (60) days before effective termination or the expiry of its authorization, whichever occurring first.
c. Advertise its intention to terminate its TSP-CA activities within at least sixty (60) days before effective termination or the expiry of its authorization, whichever occurring first, in daily newspapers, or by such other mediums and in the manner the intermediate CA PKI GB may determine.
d. Make reasonable efforts to assist its subscribers with a transition to another TSP.
e. Revoke all certificates, issued by the TSP-CA, that remain unrevoked or unexpired at the end of the notice period, whether or not the subscribers have requested a revocation.
f. Undertake the necessary measures to ensure that discontinuing its operations does not cause disruption to its subscribers and relying parties.
g. Make arrangements for its records and certificates to be archived in a trustworthy manner in accordance with the present CP.
h. Make arrangements to adequately ensure the ongoing maintenance of its systems and security measures for sensitive and accurate data,
i. Comply with any such requirements, criteria, information requests or directives as may be issued by the corresponding intermediate CA PKI GB;

In case of unexpected termination of activities for TSPs under the commercial domain, the TSP shall coordinate with the AECE PKI GB to execute a plan that may enable the AECE to take over the minimum required services from the TSP.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

The TSP shall implement and document key generation procedures in accordance with the present CP.

6.1.1 CA Private Key Pair Generation

TSP-CA

TSP-CA key pairs shall be generated within the memory of an HSM certified as meeting the requirements of section 6.2.11.

The TSP-CA Key Generation Ceremony shall be video recorded and stored securely for auditing purposes. It shall be performed in presence of a quorum of authorized persons.

If the TSP-CA is an unconstrained CA, the TSP-CA Key Generation Ceremony shall be witnessed by a Qualified Auditor (i.e. a licensed WebTrust practitioner) with the aim to produce a report opinion that the TSP-CA:

- Documented its CA key generation and protection procedures in its certificate policy, and its CPS;
- Included appropriate detail in its CA Key Generation Script;

- Maintained effective controls to provide reasonable assurance that the CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its CA Key Generation Script;
- Performed, during the CA key generation process, all the procedures required by its CA Key Generation Script.
- Issue a key generation audit report as part of the independent WebTrust audit the TSP-CA undergoes

Subscribers

Subscribers key pairs shall be generated with sufficient security maintained during the key generation process and during the delivery of these keys and corresponding certificate to the subscriber. Subscriber keys shall be generated using [FIPS 186-4] approved methods.

6.1.2 Private Key Delivery to Subscribers

TSP-CA

TSP-CA keys shall be generated in the HSM in presence of a quorum including the TSP-CA PKI GB representatives and are immediately available.

Subscribers

When the TSP generates subject's key pairs, these shall be generated within the memory of cryptographic devices conforming to FIPS 140 Level 2 at minimum and shall be delivered to subscribers using secure communication channel.

6.1.3 Public Key Delivery to Certificate Issuer

The TSP RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2 of this CP.

6.1.4 CA's Public Key Provisioning to Relying Parties

The TSP should make its TSP-CA certificates available to subscribers and relying parties by publishing them in a public repository.

The TSP-CA's public keys (for issuing CAs) will be made available on the Algerian Trusted List.

6.1.5 Key Sizes

TSPs shall be conformant to section 6.1.5 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

6.1.6 Public Key Parameter Generation

The TSP shall rely on off-the-shelf implementation of key PKI functionality including public key parameters generations. The TSP private and public keys generation shall be done in compliance to the Baseline Requirements Section 6.1.6 on quality checking.

6.1.7 Key Usage Purposes

Certificates issued by the TSP-CA shall contain a key usage bit string in accordance with [RFC 5280].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Modules Standards and Controls

The TSP shall generate its TSP-CA key pairs and store their private keys within an HSM that is certified according to the rating specified in 6.2.11.

6.2.2 CA Private Key Multi-Person Control

With regards to TSP-CA private key shared control, the TSP shall implement technical and procedural mechanisms that implement the principles of dual control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with TSP-CA cryptographic hardware.

6.2.3 CA Private Key escrow

Private keys of the TSP-CA may not be escrowed.

6.2.4 CA Private key backup

The TSP-CA private keys are backed up, stored and recovered by multiple and appropriately authorized members of the TSP-CA related staff serving in trusted roles. More than one member of the TSP-CA management shall authorize key backup and shall assign personnel in writing.

A back-up of the generated key material is taken and stored under the same security measures as the primary key material.

6.2.5 CA Private key archival

Not applicable.

6.2.6 Private key transfer into or from a cryptographic module

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

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

6.2.7 Private key storage on cryptographic module

Refer to 6.2.1.

6.2.8 Method of Activating Private Keys

TSP-CA

Private keys for the TSP-CA shall be activated by a minimum of three privileged users using the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the TSP-CA HSM.

Subscribers

Subscribers are responsible for activating and protecting the access to their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

6.2.9 Method of Deactivating Private Keys

TSP-CA

Private keys for the TSP-CA shall be deactivated in situations such as:

- There is a power failure within the CA room;

- The CA HSM is operated outside the range of supported temperatures; or
- The HSM detects a security breach and deletes all key material within its internal memory.

The TSP-CA private keys may also be routinely deactivated through procedures enforcing the principles of dual control and split knowledge and involving individuals holding trusted roles.

Subscribers

Activation and deactivation of subscriber's private key depends on the type of certificate and their storage location. This shall be described in the TSP-CA CPS and subscriber's agreement or general terms and condition of use.

6.2.10 Methods of Destroying Private Keys

TSP-CA

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 TSP-CA management.

The TSP-CA keys are destroyed through documented procedures involving individuals in trusted roles. These procedures shall enforce the principle of dual control and split knowledge. The procedures shall also ensure that the TSP-CA keys are destroyed by removing permanently from any hardware modules the keys are stored on.

Subscribers

Destruction of subscriber's private key depends on the type of certificate and their storage location. This shall be described in the TSP-CA CPS and subscriber's agreement or general terms and condition of use.

6.2.11 Cryptographic Module Rating

To protect against attacks on the secure devices or HSMs including Side-Channel Attacks (e.g. timing, power consumption, EM emission, fault injection) and attacks against the random number generator secure devices and HSMs should be successfully certified/validated to [FIPS 140-2] Level 3 or [ISO 15408] Common Criteria (CC) EAL 4+ or above and protection profiles from [CEN EN 419 221] series.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

See section 5.5 of the present CP for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Period

Considering that the Subscriber certificates will be valid for a period of maximum 3 years, the TSP-CA Certificate shall have a validity of at least 3 years after the issuance of the latest Subscriber certificate, augmented with a period taking into account the TSP-CA private key usage period and re-key activities.

Before expiration of its TSP-CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, the TSP shall generate a new certificate for signing subject key pairs, and shall apply all necessary actions to avoid disruption to the operations.

6.4 Activation Data

6.4.1 Activation data generation and protection

TSP-CA

The TSP-CA activation data shall correspond to PIN and passwords that are used to activate HSMs hosting CA keys. CA keys and their activation data shall be generated in accordance with the requirements of section 6.2, using security tokens for the protection of the CA's private key.

During the key generation ceremony of a TSP-CA, trusted individuals (key custodians) shall receive their activation data. These shall be managed according to section 6.2 of the present CP.

Subscribers

The TSP-CA shall register its subscribers prior to issuing digital certificates to them.

When the TSP is responsible for the subscribers' key generation, the activation data shall be randomly generated by the CA. This activation data shall be securely delivered to the subscriber.

6.4.2 Activation Data Protection

The TSP-CA activation data used to unlock private keys shall be protected from disclosure by means of cryptographic key material management procedures documented by the TSP in its corresponding TSP CPS.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

TSP shall perform all CA and RA functions using trustworthy systems meet its own policy requirements, the present CP requirement and audit requirements from the respective PKI GB (from AGCE or AECE).

6.5.1 Specific Computer Security Technical Requirements

The TSP-CA shall be operated according to the following security controls:

- Physical access control to the TSP-CA servers shall be 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;
- Network protection, including intrusion detection systems.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Applications shall be tested, developed and implemented in accordance with industry best practice development and change management standards.

Purchased hardware or software shall be shipped or delivered in a sealed or shrink-wrapped container and be installed by trained personnel.

6.6.2 Security Management Controls

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

There shall be no other applications, hardware devices, network connections or component software, which are not part of the PKI, connected to or installed on CA hardware.

The CA and RA functionality shall be scanned for malicious code on first use and periodically afterward.

Upon installation, and at least once a week, the integrity of the CA databases shall be validated.

6.6.3 Life Cycle Security Controls

Refer to section 5.4.8.

6.7 Network security controls

The TSP shall ensure maintenance of network security, including managed firewalls and intrusion detection systems, to ensure that the CA systems are protected against denial of service and intrusion attacks.

The network shall be segmented into several zones, based on their functional, logical and physical relationship. Network boundaries shall be enforced to limit the communication between systems deployed within different zones. Components shall be hardened so that only the services, protocols, ports, and communications that the CA has identified as necessary to its operations are activated.

6.8 Time-stamping

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

7 Certificates and CRL Profiles

This section is used to specify the Certificate and CRL formats. This includes information on profiles, versions, and extensions used.

7.1 Certificate Profile

TSP-CA

The certificate profiles that the TSP-CA shall comply to the present CP and managed by the PMA.

Subscribers

The TSP shall document the profiles of the certificates its issues in the TSP CA CPS. The TSP shall base its certificate profiles on the certificate types accepted by this CP.

7.1.1 Government Domain TSPs

7.1.1.1 Government TSP Issuing CA (Technically Constrained)

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

					then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[108]** Months	Suggested validity is 9 years as per key changeover rules
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 hash of the issuer CA public key	
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.agce.dz	OCSP responder URL
AccessMethod		M	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		M	S	http://ca.pki.agce.dz/repository/cert/government_ca_1.p7b	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ca.pki.agce.dz/repository/crl/government_ca.crl	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
clientAuthentication		O	S	True	
NameConstraints	True	M	D		MUST be present if the emailProtection is presents in the EKU
permittedSubtrees		M/O	D	<Allowed values for: Directory Name and/or rfc822Name >	Applies to both Subject DN and Subject Alternative Names.
excludedSubtrees		M/O	D	<Excluded values for: Directory Name and/or rfc822Name >	
Policy Properties					
CertificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.2.1.1	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.agce.dz/repository/cps	
BasicConstraints	True	M	S		
CA		M	S	True	TRUE for CA Certificates
pathLenConstraint		O	S	0	

7.1.1.2 Government TSP Issuing CA (Unconstrained)

Note: This profile is exclusively dedicated to AGCE TSP to issue AGCE issuing CAs certificates used to issue end entities certificates for all Government domain subscribers.

Government TSP Issuing CA Certificate Profile 2					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M	S		See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Intermediate CA Signature	Intermediate CA Signature Value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE GOUVERNEMENTALE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Government CA or Government TLS CA or Government TS CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time

					until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[108]** Months	Suggested validity is 9 years as per key changeover rules
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 hash of the issuer CA public key	
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.agce.dz	OCSP responder URL
AccessMethod		M	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		M	S	http://ca.pki.agce.dz/repository/cert/government_ca_	Issuing CA Certificate/Chain

				1.p7b or http://ca.pki.agce.dz/repository/cert/government-tls_ca.p7b or http://ca.pki.agce.dz/repository/cert/government-ts_ca.p7b	download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ca.pki.agce.dz/repository/crl/government_ca.crl or http://ca.pki.agce.dz/repository/cert/government-tls_ca.crl or or http://ca.pki.agce.dz/repository/cert/government-ts_ca.crl	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
serverAuthentication		O	S	True	Issuing CA must be constrained to a single EKU A separate intermediate must be used for each use case.
clientAuthentication		O	S	True	
timeStamping		O	S	True	
Policy Properties					
CertificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.2.1.1	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	https://ca.pki.agce.dz/repository/cps	
BasicConstraints	True	M	S		

	CA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		O	S	0	

7.1.2 Commercial Domain TSPs

7.1.2.1 Commercial TSP Issuing CA (Technically Constrained)

Commercial TSP Issuing CA Certificate Profile 1					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M	S		See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Intermediate CA Signature	Issuing CA Signature Value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	AUTORITE ECONOMIQUE DE CERTIFICATION ELECTRONIQUE	UTF8 encoded
CommonName		M	S	Commercial CA or Commercial TS CA	UTF8 encoded

Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[60]** Months	Suggested validity is 5 years as per key changeover rules
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	*<OrganizationUnitName of the issuing CA>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 hash of the issuer CA public key	
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.aece.dz	OCSP responder URL

	AccessMethod		M	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		M	S	http://pki.aece.dz/repository/cert/commercial_ca.p7b	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.aece.dz/repository/crl/commercial_ca.crl	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of subjectPublicKey	
Key Usage Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
ExtendedKeyUsage		False	M			MUST be present if the CA is technically constrained
	clientAuthentication		O	S	True	Issuing CA must be constrained to a single EKU A separate intermediate must be used for each use case.
	timeStamping		O	S	True	
NameConstraints		True	O			Must be present if the serverAuthentication is presents in the EKU
	permittedSubtrees		M/O	D	<Allowed values for: Directory Name and/or rfc822Name ; DNS Name; IP Addresses >	Applies to both Subject DN and Subject Alternative Names.
	excludedSubtrees		M/O	D	<Excluded values for: Directory Name and/or rfc822Name ; DNS Name; IP Addresses >	

Policy Properties					
CertificatePolicies	False				
PolicyIdentifier		M	S	2.16.12.3.3.1.1	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	https://pki.aece.dz/repository/cps	
BasicConstraints	True	M			
CA		M	S	True	TRUE for CA Certificates
pathLenConstraint		O	S	0	

7.1.3 Natural Person, Devices an Legal Person Certificates for Government Domain

7.1.3.1 TSA Response Signing Certificate Profile

TSA 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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements".

					PrintableString, size 2 (rfc5280)
OrganizationName		M	D	<OrganizationName of the issuing CA>	UTF8 encoded
CommonName		M	D	<CommonName of the issuing CA>	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[60]** Months	Suggested validity for the TSA certificate is maximum 5 years (calculated based on rekey period of the subordinate issuing CA)
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	<OrganizationName of the Timestamp Authority>	UTF8 encoded
StateOrProvinceName		O	D	<StateOrProvince of the Timestamp Authority>	UTF8 encoded
CommonName		M	D	<CommonName of the Timestamp Authority>	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 3072 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except

					for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuing CA's public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
digitalSignature		M	S	True	
extKeyUsage	True	M			
timeStamping		M	S	True	
Policy Properties					
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	

certificatePolicies		False	M			
	policyIdentifier		M	D	<PolicyIdentifier of the issuing TSA PS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the TSA PS>	
certificatePolicies		False				
	policyIdentifier		M	S	2.23.140.1.4.2	BR CS Reserved OID (TSA)

7.1.3.2 Verification Response Signing Certificate Profile

Verification 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	Issuing CA's Signature.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[36]** Months	
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the signature verification service certificate>*	UTF8 encoded
StateOrProvinceName		O	D	*<StateOrProvince of the signature verification service certificate>*	UTF8 encoded
CommonName		M	D	*<CommonName of the signature verification service certificate>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash of the Issuing CA's public key	When this extension is used, this field

					MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
digitalSignature		M	S	True	
Policy Properties					
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the signature verification service certificate>	

7.1.3.3 SSL (Web Server) Certificate Profile

SSL Server 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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing 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 + not more than **[397]** Days	Maximum 397 days validity allowed (BR SSL requirement)
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the SSL certificate >*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the SSL certificate>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the SSL certificate>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the SSL certificate>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA/ECDSA	
SubjectPublicKey		M	D	Public 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 Issuing CA’s public key	When this extension is used, this field MUST be supported as a minimum

AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
	AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
SubjectAltName		False	M	D	Allocated as per certificate request	Either Domain name(s) or Public IP address(es) that are applicable, linked to the subject common name field
	dnsName		O/M	D	<fully qualified domain name>	
	ipAddress		O/M	D	<public IP address>	
Key Usage Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
	keyEncipherment		M	S	True	For ECDSA algorithm this key usage is not permitted
extKeyUsage		False	M			
	id-kp-serverAuth		M	S	True	
	clientAuth		O	S	True	

Policy Properties					
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the SSL certificate>	
certificatePolicies	False	M			
policyIdentifier		M	S	2.23.140.1.2.2	CA/B Forum Policy OID for OV SSL certificates
basicConstraints	True	O	S	False	

7.1.3.4 VPN Certificate Profile

VPN 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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption

Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than [397] Days	Maximum 397 days validity allowed (SSL BR requirements)
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the VPN certificate >*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the VPN certificate>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the VPN certificate>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.

CommonName		M	D	*<CommonName of the VPN certificate>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA/ECDSA	
SubjectPublicKey		M	D	Public 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 Subordinate Issuing CA's public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
SubjectAltName	False	M	D	Allocated as per certificate request	Either Domain name(s) or Public IP address(es) that

					are applicable, linked to the subject common name field
dnsName		O/M	D	<fully qualified domain name>	dnsName
ipAddress		O/M	D	<public IP address>	ipAddress
Key Usage Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
keyEncipherment		M	S	True	For ECDSA algorithm this key usage is not permitted
extKeyUsage	False	M			
id-kp-serverAuth		M	S	True	
Policy Properties					
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
policyIdentifier		M	D	<PolicyIdentifier of the VPN certificate>	
certificatePolicies	False	M			
policyIdentifier		M	S	2.23.140.1.2.2	CA/B Forum Policy OID for OV SSL certificates
basicConstraints	True	O	S	False	

7.1.3.5 Devices (SSL Client Authentication) Certificate Profile

Devices (SSL Client 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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than [397] Days	Maximum 397 days validity allowed (SSL BR requirements)
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	*<OrganizationName of the devices (client*	UTF8 encoded

				authentication) certificate>	
LocalityName		M/O	D	*<LocalityName of the devices (client authentication) certificate>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the devices (client authentication) certificate>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the devices (client authentication) certificate>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA/ECDSA	
SubjectPublicKey		M	D	Public Key length: 2048 or 4096 (RSA)/256 or 384 (ECDSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuing CA's public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
SubjectAltName		False	M	D	Allocated as per certificate request	Either Domain name(s) or Public IP address(es) that are applicable, linked to the subject common name field
	dnsName		O/M	D	<fully qualified domain name>	dnsName
	ipAddress		O/M	D	<public IP address>	ipAddress
Policy Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
extKeyUsage		False	M			
	id-kp-serverAuth		M	S	True	
	id-kp-clientAuth		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	policyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	policyIdentifier		M	D	<PolicyIdentifier of the devices (client authentication) certificate>	

certificatePolicies	False	M	S		
policyIdentifier		M	S	2.23.140.1.2.2	CA/B Forum Policy OID for OV SSL certificates
basicConstraints	True	O	S	False	

7.1.3.6 Qualified Signing Certificate Profile

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	Issuing CA's Signature.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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)
OrganizationUnitName		O	D	*<OrganizationUnitName of the issuing CA>*	UTF8 encoded

OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	*<OrganizationUnitName of the individual>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the individual>*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the individual>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the individual>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the individual>*	UTF8 encoded

SERIALNUMBER		O	D	*<Unique Identifier for each individual as constructed by the RA>*	PrintableString encoded
GivenName[3]		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			
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			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP

[3] The givenName/surname attribute has a usage purpose that is different from the required choice of commonName. commonName is used for user friendly representation of the person's name, whereas givenName/surname is used where more formal representation or verification of specific identity of the user is required.

crlDistributionPoints	False	M			
DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
nonrepudiation		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
PolicyIdentifier		M	D	<PolicyIdentifier for the certificates issued to individuals for qualified signing in local>	

7.1.3.7 Qualified Remote Signing Certificate Profile

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	Issuing CA's Signature.	Issuing CA's signature value
TBSCertificate					
Version	False	M			

Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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)
OrganizationUnitName		O	D	*<OrganizationUnitName of the issuing CA>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing 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	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

OrganizationUnitName		O	D	*<OrganizationUnitName of the individual>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the individual>*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the individual>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the individual>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the individual>*	UTF8 encoded
SERIALNUMBER		O	D	*<Unique Identifier for each individual as constructed by the RA>*	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			
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			Mandatory in all certificates except for self-signed certificates

	KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
	AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	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			
	nonrepudiation		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier for the certificates issued to	

					individuals for Qualified Remote signing>	

7.1.3.8 Advanced Signing Certificate Profile

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.	Issuing CA signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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)
OrganizationUnitName		O	D	*<OrganizationUnitName of the issuing CA>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	D	*<CommonName of the issuing CA>*	UTF8 encoded

Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	*<OrganizationUnitName of the individual>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the individual>*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the individual>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the individual>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the individual>*	UTF8 encoded
SERIALNUMBER		O	D	<Unique Identifier for each individual as constructed by the RA>	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			
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			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
	nonrepudiation		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier of the certificates issued to individuals for advanced signing>	

7.1.3.9 Authentication Certificate Profile

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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption

Issuer	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	<OrganizationUnitName of the issuing CA>	UTF8 encoded
OrganizationName		M	D	<OrganizationName of the issuing CA>	UTF8 encoded
CommonName		M	D	<CommonName of the issuing CA>	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	*<OrganizationUnitName of the individual>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the individual>*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the individual>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.

StateOrProvinceName		M/O	D	*<StateOrProvince of the individual>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the individual>*	UTF8 encoded
SERIALNUMBER		O	D	*<Unique Identifier for each individual as constructed by the RA>*	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			
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			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field

	AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
	AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		MO	D	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	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			
	digitalSignature		M	S	True	
extKeyUsage		False	M			
	id-kp-clientAuth		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier of the authentication certificate>	

7.1.3.10 eSeal/Government Entity's Signing Certificate Profile

eSeal/Government Entity's 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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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)
OrganizationUnitName		O	D	<OrganizationUnitName of the issuing CA>	UTF8 encoded
OrganizationName		M	D	<OrganizationName of the issuing CA>	UTF8 encoded
CommonName		M	D	<CommonName of the issuing CA>	UTF8 encoded
Validity	False	M			Implementations MUST specify

					using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationUnitName		O	D	*<OrganizationUnitName of the eSeal certificate>*	UTF8 encoded
OrganizationName		M	D	*<OrganizationName of the eSeal certificate >*	UTF8 encoded
LocalityName		M/O	D	*<LocalityName of the eSeal certificate>*	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
StateOrProvinceName		M/O	D	*<StateOrProvince of the eSeal certificate>*	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	*<CommonName of the eSeal certificate>*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
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			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	D	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	D	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	D	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
digitalSignature		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	D	<PolicyIdentifier of the issuing CA CPS>	

	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	PolicyIdentifier		M	D	<PolicyIdentifier of the eSeal certificate>	

7.1.4 Natural Person, Devices an Legal Person Certificates for commercial domain

7.1.4.1 Advanced Signing Certificate Profile

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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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	*< Organization Name of the issuing CA >*	UTF8 encoded
CommonName		M	S	*< CommonName of the issuing CA >*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CommonName		M	D	*< Concatenation of given name and surname as in government-issued ID card separated by a "space" character – Sign >*	UTF8 encoded
GivenName		M	D	*< Given name of the individual as in government-issued ID card >*	UTF8 encoded
Surname		M	D	*< Surname name of the individual as in government-issued ID card >*	UTF8 encoded
OrganizationName		M	D	*< Organization Name whom the individual belongs >*	UTF8 encoded

OrganizationUnitName		O	D	*< Organization Unit Name whom the individual belongs >*	UTF8 encoded
Title		M	D	*< Job title as mentioned in the job certificate delivered by the organization >*	UTF8 encoded
Email		M	D	*< Professional Email Address of the individual >*	UTF8 encoded
LocalityName		M	D	*< Locality Name of Organization Area >*	UTF8 encoded.
StateOrProvinceName		M	D	*<State Or Province of Organization Area>*	UTF8 encoded.
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
Serial Number		M	D	*< SHA256 hash computed value of national identification number (NIN) (for citizen) or SHA256 hash computed value of <PAS_Country Code-Passport Number> (for Visitor/ Expat) >*	UTF8 encoded For country code : Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
Organization Identifier		M	D	*< RC: Organization Commercial Registration Number Or AGR: agreement Number, NIF: Organization TAX identification number >*	UTF8 encoded
UID		O	D	*< SHA256 hash computed value based on certificate's subject DN given by issuing CA >*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	

SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	S	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
DigitalSignature		M	S	True	
Extended Key Usage Properties					
Extended keyUsage	False	M			
Document Signing		M	S	True	

Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.3.1.2	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
PolicyIdentifier		M	S	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:userNotice		O	S	Advanced Signing Certificate	
BasicConstraints	False	M			
End Entity		M	S	True	TRUE for End Entity Certificates

CE[2] = Critical Extension

O/M[3]: O = Optional M = Mandatory
CO[4] = Content: S =Static, D = Dynamic

7.1.4.2 Qualified Signing Certificate Profile

Qualified Signing Certificate Profile (Natural Person)					
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.	Issuing CA's Signature Value
TBSCertificate					
Version	False	M			

Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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	*< OrganizationUnitName of the issuing CA >*	UTF8 encoded
CommonName		M	S	*< CommonName of the issuing CA >*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CommonName		M	D	*< Concatenation of given name and surname as in government-issued ID card separated by a "space" character > – Qsign*	UTF8 encoded

GivenName		M	D	*< Given name of the individual as in government-issued ID card >*	UTF8 encoded
Surname		M	D	*< Surname name of the individual as in government-issued ID card >*	UTF8 encoded
OrganizationName		M	D	*< Organization Name whom the individual belongs >*	UTF8 encoded
OrganizationUnitName		O	D	*< Organization Unit Name whom the individual belongs >*	UTF8 encoded
Title		M	D	*< Job title as mentioned in the job certificate delivered by the organization >*	UTF8 encoded
Email		M	D	*< Professional Email Address of the individual >*	UTF8 encoded
LocalityName		M	D	*< Locality Name of Organization Area >*	UTF8 encoded.
StateOrProvinceName		M	D	*< State Or Province of Organization Area >*	UTF8 encoded.
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
Serial Number		M	D	*< SHA256 hash computed value of national identification number*	UTF8 encoded For country code : Encoded according

				(NIN) (for citizen) or SHA256 hash computed value of <PAS-Country Code- Passport Number> (for Visitor/ Expat) >	to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
Organization Identifier		M	D	*< RC: Organization Commercial Registration Number Or AGR: agreement Number, NIF: Organization TAX identification number >*	UTF8 encoded
UID		O	D	*< SHA256 hash computed value based on certificate's subject DN given by issuing CA >*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
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			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	S	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			

DistributionPoint		M	S	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
DigitalSignature		M	S	True	
nonrepudiation		M	S	True	
Extended Key Usage Properties					
Extended keyUsage	False	M			
Document Signing		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
PolicyIdentifier		M	S	<PolicyIdentifier for the certificates issued to individuals for qualified signing in local>	
policyQualifiers:userNotice		O	S	Qualified Signing Certificate	
BasicConstraints	False	M			
End Entity		M	S	True	TRUE for End Entity Certificates

CE[2] = Critical Extension O/M[3]: O = Optional M = Mandatory CO[4] = Content: S =Static, D = Dynamic

7.1.4.3 Qualified Authentification and Signing Certificate Profile

Qualified Authentication and Signing Certificate Profile (Natural Person)					
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.	Issuing CA's Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	S	Issuing CA's Signature.	UTF8 encoded

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject		False	M			
CommonName			M	D	*< Concatenation of given name and surname as in government-issued ID card separated by a "space" character >- QID*	UTF8 encoded
GivenName			M	D	*< Given name of the individual as in government-issued ID card >*	UTF8 encoded
Surname			M	D	*< Surname name of the individual as in government-issued ID card >*	UTF8 encoded
OrganizationName			M	D	*< Organization Name whom the individual belongs >*	UTF8 encoded
OrganizationUnit			O	D	*< Organization Unit Name whom the individual belongs >*	UTF8 encoded

Title		M	D	*< Job title as mentioned in the job certificate delivered by the organization >*	UTF8 encoded
Email		M	D	*< Professional Email Address of the individual >*	UTF8 encoded
LocalityName		M	D	*< Locality Name of Organization Area >*	UTF8 encoded.
StateOrProvinceName		M	D	*< State Or Province of Organization Area >*	UTF8 encoded.
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
Serial Number		M	D	*< SHA256 hash computed value of national identification number (NIN) (for citizen) or SHA256 hash computed value of <PAS-Country Code- Passport Number> (for Visitor/ Expat) >*	UTF8 encoded For country code : Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
Organization Identifier		M	D	*< RC: Organization Commercial Registration Number Or AGR: agreement Number, NIF: Organization TAX identification number >*	UTF8 encoded
UID		O	D	*< SHA256 hash computed value based on certificate's subject DN given by issuing CA >*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except

					for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	S	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
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			
DigitalSignature		M	S	True	
nonrepudiation		M	S	True	
Extended Key Usage Properties					
Extended keyUsage	False	M			
Document Signing		M	S	True	
id-kp-clientAuth		M	S	True	
SmartCardLogon		M	S	True	
Policy Properties					
certificatePolicies	False	M			

	PolicyIdentifier		M	S	<PolicyIdentifier of the issuing CA CPS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	S	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<PolicyIdentifier for the certificates issued to individuals for qualified Authentification and signing in local>	
	policyQualifiers:userNotice		O	S	Qualified ID Signing Certificate	
BasicConstraints		False	M			
	End Entity		M	S	True	TRUE for End Entity Certificates

CE[2] = Critical Extension O/M[3]: O = Optional M = Mandatory CO[4] = Content: S =Static, D = Dynamic

7.1.4.4 Authentication Certificate Profile

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.	Issuing CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.

Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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	*<OrganizationName of the issuing CA>*	UTF8 encoded
CommonName		M	S	*<CommonName of the issuing CA>*	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CommonName		M	D	*< Concatenation of given name and surname as in government-issued ID card separated by a "space" character >– Auth*	UTF8 encoded
GivenName		M	D	*< Given name of the individual as in government-issued ID card >*	UTF8 encoded

Surname		M	D	*Surname name of the individual as in government-issued ID card >*	UTF8 encoded
OrganizationName		M	D	*< Organization Name whom the individual belongs >*	UTF8 encoded
OrganizationUnitName		O	D	*< Organization Unit Name whom the individual belongs >*	UTF8 encoded
Title		M	D	*< Job title as mentioned in the job certificate delivered by the organization >*	UTF8 encoded
Email		M	D	*< Professional Email Address of the individual >*	UTF8 encoded
LocalityName		M	D	*<Locality Name of Organization Area >*	UTF8 encoded.
StateOrProvinceName		M	D	*< State Or Province of Organization Area >*	UTF8 encoded.
CountryName		M	S	DZ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
Serial Number		M	D	*< SHA256 hash computed value of national identification number (NIN) (for citizen) or SHA256 hash computed value of <PAS-Country Code- Passport Number> (for Visitor/ Expat) >*	UTF8 encoded For country code : Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
Organization Identifier		M	D	*< RC: Organization Commercial Registration Number Or AGR:*	UTF8 encoded

				agreement Number, NIF: Organization TAX identification number >	
UID		O	D	*< SHA256 hash computed value based on certificate's subject DN given by issuing CA >*	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
AccessMethod		M	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		M	S	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			

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			
DigitalSignature		M	S	True	
Extended Key Usage Properties					
Extended keyUsage	False	M			
id-kp-clientAuth		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	<PolicyIdentifier of the issuing CA CPS>	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	S	<HTTP URL of the issuing CA CPS>	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.12.3.1.4.1.1	
policyQualifiers:userNotice		O	S	Authentication Certificate	
BasicConstraints	False	M			
End Entity		M	S	True	TRUE for End Entity Certificates

7.1.4.5 eSeal/Commercial Entity's Signing certificate Profile

eSeal/Commercial Entity's 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.	Issuing CA's Signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			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	<OrganizationName of the issuing CA>	UTF8 encoded
CommonName		M	S	<CommonName of the issuing CA>	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	

NotAfter		M	D	Certificate generation process date/time + up to **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False	M			
CommonName		M	D	*< Business Name > - QeSeal*	UTF8 encoded
OrganizationName		M	D	*<Organization Name >*	UTF8 encoded
OrganizationUnitName		O	D	*< Organization Unit Name >*	UTF8 encoded
Email		M	D	*< Professional Email Address of Organization >*	UTF8 encoded
LocalityName		M	D	*< Locality Name of Organization Area >*	UTF8 encoded.
StateOrProvinceName		M	D	*< State Or Province of Organization Area >*	UTF8 encoded.
CountryName		M	S	DZ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
Organization Identifier		M	D	*< RC: Organization Commercial Registration Number Or AGR: agreement Number, NIF: Organization TAX identification number >*	UTF8 encoded
dnQualifier		O	D	*< SHA256 hash computed value based on certificate's subject DN given by issuing CA >*	UTF8 encoded
SubjectPublicKeyInfo	False	M			

	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			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	<HTTP URL of the issuing CA OCSP Service>	OCSP responder URL
	AccessMethod		M	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		M	S	<HTTP URL of the issuing CA PKCS7 file>	Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	<HTTP URL of the issuing CA CRL file>	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	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			
	DigitalSignature		M	S	True	
	nonrepudiation		M	S	True	

Extended Key Usage Properties						
Extended keyUsage		False	M			
	Document Signing		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<PolicyIdentifier of the issuing CA CPS>	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	S	<HTTP URL of the issuing CA CPS>	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<PolicyIdentifier of the eSeal certificate>	
	policyQualifiers:userNotice		O	S	Qualified eSeal Certificate	
BasicConstraints		False	M			
	End Entity		M	S	True	TRUE for End Entity Certificates

CE[2] = Critical Extension O/M[3]: O = Optional M = Mandatory CO[4] = Content: S =Static, D = Dynamic

7.2 CRL Profile

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.	CA's signature value

TbSCertList	False				
Version	False	M			
Version		M	S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	DZ	
OrganizationName		M	D	<OrganizationName of the CA>	UTF8 encoded
CommonName		M	D	<CommonName of the CA>	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + **[1]** day + 2 hours	
RevokedCertificates	False	O			
Certificate		M	D		
CertificateSerialNumber		M	D	Serial number of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	False	O			
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					
AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of subjectPublicKey of the 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	Issuing CA Certificate/Chain download URL over HTTP	

7.3 OCSP Profile

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

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

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

8 Compliance Audit and Other Assessments

Regarding the provision of TSP-CA services and related activities, it is the duty of the corresponding intermediate CA PKI GB to ensure the TSP meets the requirements, standards, procedures and service levels according to the CP and other controls agreed upon between the intermediate CA PKI GB and the TSP.

Frequency and circumstances of compliance verification are defined by the intermediate CA PKI GB and approved by the PMA. The intermediate CA PKI GB may conduct the compliance verification directly with the TSP or appoint an auditor to do the verification on their behalf.

In case of unconstrained TSP CA, an external audit shall be conducted by an independent WebTrust practitioner according to the WebTrust audit scheme. The audit is organized on a yearly basis in close coordination with the intermediate PKI GB.

The intermediate CA PKI GB evaluates the results of the audit and/or compliance verification then accordingly defines the required measures that should be taken by the TSP regarding its TSP-CA in order to rectify the situation and ensure compliance.

If the proposed measures are not timely and sufficiently implemented by the TSP regarding its TSP-CA, the intermediate CA PKI GB may decide to cancel the agreement and revoke the respective TSP-CA(s) certificates.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance of Renewal Fees

The TSP may charge fees for certificate issuance and renewal. Details with regard to fees shall be documented in the corresponding TSP's CPS.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance coverage

Each PKI Participant, except the Relying Parties, will maintain appropriate insurance to meet its obligations under the present CP and will maintain a sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

The TSP shall provide details about fees in its TSP-CA CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The TSP shall guarantee the confidentiality of any classified data. This shall include the following types of data:

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

9.3.2 Information not within the scope of confidential information

Any information not defined as confidential by the TSP shall be deemed public. This includes the information published on the TSP's repository.

9.3.3 Responsibility to protect confidential information

The TSP shall protect confidential information through training and policy enforcement with its employees, contractors and suppliers.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

The TSP shall observe personal data privacy rules and privacy rules as specified in the present CP. The TSP shall implement these provisions across all RAs under its responsibility.

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 TSP trusted personnel may be permitted to access subscribed private information for the purpose of certificate lifecycle management.

The TSP shall respect 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 TSP to subscribers except for information about themselves and only covered by the contractual agreement between the TSP and the subscriber.

The TSP may not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the TSP releases private information, this information may not be used for any purpose apart from the requested purposes. Parties granted access shall secure the private data from compromise, and refrain from using it or disclosing it to third-parties. Also, these parties are bound to observe personal data privacy rules in accordance with the relevant laws in Algeria.

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

- The communications between the TSP-CA RA systems and the subscriber;
- Sessions to deliver certificates.

Next to the information retained by the TSP with regards to its TSP-CA activities, information pertaining to the subscribers' certificates can also be retained by the RA.

9.4.2 Information treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to protect private information

The TSP employees and contractors shall handle personal information in strict confidence under the TSP contractual obligations that should be at least as protective as the terms specified in section 9.4.1.

9.4.5 Notice and consent to use private information

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

9.4.6 Nondisclosure Pursuant Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The TSP may own and reserve all intellectual property rights associated with its own databases, web sites, the CAs' digital certificates and any other publication whatsoever originating from the PKI, including the present CP.

When the TSP uses software from third party suppliers, it shall ensure that intellectual property rights of the supplier are maintained. This shall be defined in the supplier's license agreement.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The TSP shall warrant that their procedures are implemented in accordance with this CP and the corresponding TSP CPS, and that any certificates issued under the TSP CPS are in accordance with the stipulations specified.

9.6.2 RA Representations and Warranties

The TSP shall warrant that it performs RA functions as per the stipulations specified in the TSP CPS.

9.6.3 Subscriber Representations and Warranties

The TSP shall warrant that each subscriber signs a subscriber's agreement with the TSP that lists the subscriber's obligations. The TSP shall use its own CPS to convey legal conditions of usage of certificates to subscribers.

9.6.4 Relying parties Representations and Warranties

The TSP shall use its own CPS to convey conditions of usage of certificates to be honoured by relying parties.

9.6.5 Representations and Warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

TSPs may not disclaim any responsibilities or obligations described in this CP. Any such disclaimers of warranties shall be documented in the TSP's CPS and reviewed/validated by the relevant PKI GB (from AGCE or AECE) depending on whether the TSP CAs are established under the Government CA or Commercial CA.

9.8 Limitations of Liability

The total liability of the TSP CAs may be limited provided that TSP operations remain compatible with the provisions of this TSP CP. Such limitations of liability shall be documented in the TSP's CPS and reviewed/validated by the relevant PKI GB (from AGCE or AECE) depending on whether the TSP CAs are established under the Government CA or Commercial CA.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

The present TSP CP is approved by the PMA and shall remain in force until amendments are published on the PMA repository and relevant communication towards TSPs occurred through the PKI GB (from AGCE or AECE).

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The PMA shall coordinate with the PKI GBs (from AGCE and AECE) the communication that will be executed towards the TSPs in relation to the termination (and related effects) of this TSP CP.

9.11 Individual notices and communications with participants

Notices related to the present TSP CP may be addressed by TSPs to the respective PKI GB from AGCE or AECE. 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.

Notices and communications related to the present TSP CP may be addressed to TSPs from their RA or relying parties. The TSPs CPSs shall document the relevant communications procedures and channels.

For all other communications, no further stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The TSP CP shall be reviewed at least once a year by the PMA. Suggested amendments are discussed with the PKI GBs from AGCE and AECE. The final agreed amendments are approved and applied by the PMA. The newer version of the CP is marked by an indicated new version of the document.

9.12.2 Notification Mechanism and Period

Upon publishing on the PMA repository, the newer version of the CP becomes effective. The older versions of this CP are archived by the PMA on its repository. The PMA shall coordinate with the PKI GBs from AGCE

and ARPCE the communication that will be executed towards the TSPs in relation to the amendments of this TSP CP and related effects.

9.12.3 Circumstances Under Which OID Must be Changed

Major changes to this TSP CP that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the CP OID or CP pointer qualifier (URL). The PMA shall coordinate proper communication to TSPs through the PKI GBs from AGCE and AECE.

9.13 Dispute Resolution Procedures

The PKI GBs from AGCE and AECE shall facilitate dispute resolution between PKI participants when conflicts arise as a result of the use of certificates issued under this TSP CP.

9.14 Governing Law

The laws of the Republic of Algeria shall govern the enforceability, construction, interpretation, and validity of the present CP.

9.15 Compliance with applicable law

The present CP claims compliance to applicable laws of the Republic of Algeria, in particular [Law 15-04] and [Decree 16-135]. A TSP shall comply to the same laws at minimum and any relevant provisions related to the sector in which the TSP is operating. TSPs shall communicate with the respective PKI GB from AGCE or AECE to establish such compliance requirements and shall document these in their respective TSP CAs CPSs.

9.16 Miscellaneous provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

TSPs complying to the provisions of this TSP CP may not assign their rights, duties or obligations without the prior written consent of the respective PKI GB (AGCE or AECE).

9.16.3 Severability

If any provision of this TSP CP is determined to be invalid or unenforceable, the other sections shall remain in effect until this CP is updated.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.