ECONOMIC AUTHORITY OF ELECTRONIC CERTIFICATION

AECE PKI

PKI Disclosure Statement

Version 1.1

JANUARY 2021

Document management

Information

Group of document	AECE
Title	PKI Disclosure Statement
Project reference	Algeria National PKI
Annex	n.a.

Version control

Version	Date	Description / Status	Responsible
V0.1	15/01/2020	Initial document preparation	AECE
1.0	20/01/2021	Released with alignment to latest AECE CP/CPS	AECE
1.1	31/01/2021	Feedback from the PKI Governance Board	AECE

Document Signoff

Version	Date	Responsible	Validated by	Reviewed and Approved by
V 1.1	31/01/2021	AECE	AECE PKI GB 31/01/2021	AECE PKI GB 31/01/2021

Table of contents

1 Overview 4
2 Purpose 5
3 Contact information 5
4 Definitions 5
5 Compliance 6
6 Certificate Type, Validation Procedures and Usages 6
7 Obligations 6
8 Certificate Status Checking Obligations of Relying Parties 7
9 Limited Warranty and Disclaimer/Limitation of Liability 7
10 Applicable Agreements, CP, CPS 8
11 Privacy Policy 8
12 Refund Policy 8
13 Applicable Law and Dispute Resolution 8
14 CA and Repository Licenses, Trust Marks, and Audit 8

1 Overview

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 Trust Service Providers (TSP) offering digital certification and trust services to government and non-government entities.

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

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

The Algerian Government tasked the Post and Electronic Communication Regulation Authority (Autorité de Régulation de la Poste et des Communications Électroniques - ARPCE) to oversee the establishment of TSPs under the Commercial PKI branch. In this context, the ARPCE operates as the Authority for Commercial Certification (Autorité Economique de Certification Electronique – AECE). The AECE implements and operates the COM-CA as an intermediate CA certified by the NR-CA. The overall mandate of the AECE is to license and supervise the operations of organizations offering certification and trust services to be certified by the COM-CA.

The governance structure of the AECE PKI is referred to as the AECE PKI Governance Board (AECE PKI GB). It interacts closely with the PMA to implement the COM-CA operational cycle.

The abbreviations ARPCE and AECE will be used interchangeably hereinafter.

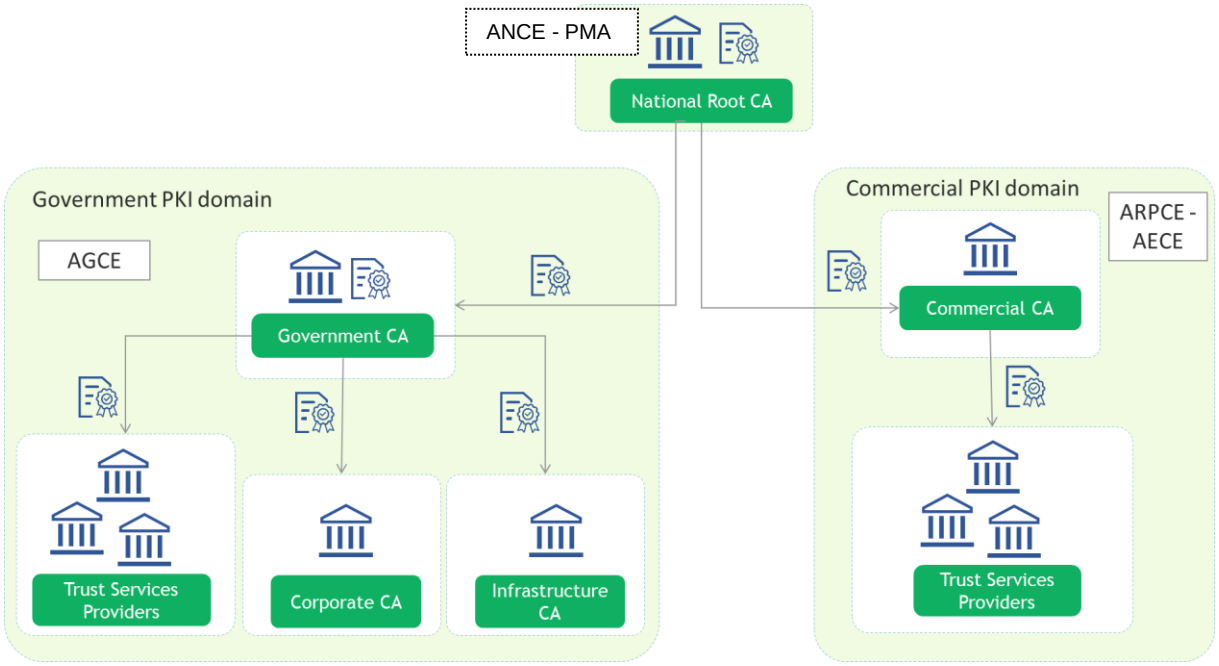

Figure 1: The Algerian National PKI hierarchy

2 Purpose

This document is the PKI Disclosure Statement of the AECE in delivering its certification services to subscribers and relying parties. The purpose of this document is to summarize and present the AECE key services in a more readable and understandable format for the benefit of Subscribers and Relying Parties.

3 Contact information

AECE can be contacted in relation to its offered services at the following address:

Autorité Economique de Certification Electronique

Cyber Park Sidi Abdellah, BT D,

Rahmania, Zeralda, Alger

Tel: +213 (0) 21 47 02 05

+213 (0) 21 47 77 77

Fax: +213 (0) 21 47 01 97

Email: Info@aece.dz

Certificate Problem Report

Subscribers, relying parties and other third parties can report suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to any certificates issued by AECE COM-CA by sending an email to reports@aece.dz.

4 Definitions

The following definitions are used throughout this agreement

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

"Certificate Application" means a request to a CA for the issuance of a Certificate.

"Certification Authority" or **"CA"** An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both COM-CA and Subordinate CAs.

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

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

"Intellectual Property Rights" means any and all now known or hereafter existing rights associated with intangible property, including, but not limited to, registered and unregistered, trademarks, trade dress, trade names, corporate names, logos, inventions, patents, patent applications, software, know-how and all other intellectual property and proprietary rights (of every kind and nature throughout the universe and however designated).

"Public Key Infrastructure" or **"PKI"** means in the context of this PDS the public key infrastructure operated by the AECE and governed by the COM-CA CP/CPS.

"Relying Party" A recipient of a certificate who acts in reliance on that certificate/digital signatures verified using that certificate

"Repository" A trustworthy system for storing and retrieving certificates or other information relevant to certificates

"Services" mean, collectively, the digital certificate service and any collateral product, benefit, or utility that AECE makes available to subscribers and relying parties.

"Subscriber" A subject who is issued a certificate.

"**Trust Service Provider**" or "**TSP**" means organizations that operate certification services under the COM CA.

5 Compliance

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

Relying Parties and Subscribers shall comply with the provisions of the Privacy policies specified later in this document.

6 Certificate Type, Validation Procedures and Usages

The AECE oversees the establishment of commercial Trust Service Providers (TSP). The AECE operates the Commercial CA (COM-CA) and offers the following related services to its subscribers:

- Certificate enrolment, certificate requests and revocation requests through the AECE RA function;
- Certificate issuance and revocation services;
- Certificate Revocation Lists (CRL) issuance and publishing on AECE public repository;
- Online certificate Status Protocol (OCSP) services and responses;
- Helpdesk service to respond to certificate problem requests.

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

A subscriber shall meet its contractual obligations with the AECE and will undergo an enrolment process as documented in the COM-CA CPS.

7 Obligations

It is the responsibility of the AECE to:

- Ensure that the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the COM-CA keys and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key;
- Generate CA private keys using multi-person control "m-of-n" split key knowledge scheme;
- Backing up of CA signing Private Keys under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control, procedures for all such personal secrets;
- Maintain the integrity of the COM-CA operations at all times;
- Provide certificate status validation mechanisms, such as CRLs and OCSP services as applicable; and
- Conduct regular compliance audits and assessments as described in the COM-CA CP/CPS.

8 Certificate Status Checking Obligations of Relying Parties

If a Relying Party is to reasonably rely upon a certificate issued by the COM-CA, it shall:

- Agree to and accept the terms and conditions specified in the Relying Party obligations specified in the relevant CA CPS;
- Ensure that the reliance is restricted to appropriate uses as defined in the relevant CPS document, by checking its key usage field extensions;
- Verify the Validity by ensuring that the Certificate has not expired;
- Ensure that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determine that such Certificate provides adequate assurances for its intended use.

9 Limited Warranty and Disclaimer/Limitation of Liability

AECE is responsible for the execution of its services as specified in its CP/CPS.

AECE is not liable for :

- the secrecy of the Private Keys of Subscriber ;
- any misuse of the Subscriber' CA Certificate or for the wrong decisions of a Relying Party or any consequences due to error or omission in Certificate validation checks.

Within the limitations of the Algeria laws, AECE cannot be held liable (except in case of fraud or deliberate abuse) for:

- Profit loss ;
- Loss of data ;
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures ;
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant or if it is the result of negligence or with intent to deceive AECE, or any person receiving or relying on the certificate ;

- Any liability incurred as a result of the applicant breaking any laws applicable in Algeria, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- The failure to perform if such failure is occasioned by force majeure.

10 Applicable Agreements, CP, CPS

AECE agreements and CPSs can be found at (https://pki.aece.dz/repository).

11 Privacy Policy

AECE observes personal data privacy rules and privacy rules as specified in AECE CPS documents.

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

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

Private information will not be disclosed by the AECE to Subscribers except for information about themselves and only covered by the contractual agreement between the AECE and the Subscribers.

AECE will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the AECE releases private information, AECE will ensue through reasonable means that this information is not used for any purpose apart from the requested purposes.

All communications channels with AECE shall preserve the privacy and confidentiality of any exchanged private information.

12 Refund Policy

No refunds is applicable for any fees charged by AECE.

13 Applicable Law and Dispute Resolution

The Applicable law governing this document, its meaning and interpretation shall be the law of the people's democratic republic of Algeria.

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

14 CA and Repository Licenses, Trust Marks, and Audit

AECE ensures that its CAs and related services are subject to regular internal audits. These audits are planned and executed, at a minimum, twice a year.

External audits are planned and executed by an independent WebTrust practitioner according to the WebTrust audit scheme. These are organized on a yearly basis by the AECE and apply for the certification services offered through AECE CAs.