الجـــمـــهوريـــة الجـــزائـــريـــة الديمقـــراطية الشـــعبية

السلطة الحكومية للتصديق الالكتروني

AGCE PKI

PKI Disclosure Statement

APPROVED

Document Management

Information

Group of document	AGCE PKI
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	AGCE
V1.0	25/10/2020	Released with alignment to latest AGCE CPSs	AGCE
V1.1	08/10/2021	Released with alignment to latest AGCE CPSs	AGCE
V2.0	23/06/2022	Released with alignment to latest AGCE CPSs	AGCE
V2.1	08/06/2023	Release with alignment to latest AGCE CPSs	AGCE

Document Signoff

Version	Date	Responsible	Reviewed and Approved By
V2.1	08/06/2023	AGCE	AGCE (PKI GB)

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 8
8 Certificate Status Checking Obligations of Relying Parties 8
9 Limited Warranty and Disclaimer/Limitation of Liability 9
10 Applicable Agreements, CP, CPS 9
11 Privacy Policy 9
12 Refund Policy 10
13 Applicable Law and Dispute Resolution 10
14 CA and Repository Licenses, Trust Marks, and Audit 10

1 Overview

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

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

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

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

- **Government CAs:**

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

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

  - **Corporate CA:** will issue Digital Signature and Authentication certificates to natural persons (government employees) and legal persons (government entities).
  - **OV TLS Server CA:** will issue organization validated Server Authentication certificates to non-natural entities such as servers and VPN device certificates. It will also issue Client Authentication certificates to non-natural organization end entities (devices).
  - **SMIME CA:** will issue email protection (SMIME) certificates to natural persons (government employees).
  - **Code Signing CA:** will issue code signing certificates to legal persons (government entities).
  - **Trust services CA:** will issue timestamping certificates for AGCE and Government TSPs operating Timestamping services. It will also issue signing certificates for digital signature verification service operated by governmental TSPs.

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

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

The governance structure of the AGCE PKI is referred to as the AGCE PKI Governance Board (AGCE PKI GB). The PKI GB is composed of senior consultants appointed from PKI unit within

AGCE, it is responsible for maintaining this and other CP and CPS documents relating to certificates within AGCE PKI. It interacts closely with the PMA to implement the GOV-CA operational cycle.

2 Purpose

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

3 Contact information

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

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

Certificate Problem Report

Subscribers, relying parties, application software suppliers, and other third parties can report suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to any certificates issued by AGCE CAs by sending an email to Certification.Problem@agce.dz.

4 Definitions

The following definitions are used throughout this agreement

"Certificate" means an electronic document that uses a digital signature to connect a public key with an identity (person or organization) and, at least, states a name or identifies the issuing certificate authority, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing certificate authority.

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

"Certification Authority" or **"CA"** means an entity authorized to issue, suspend, or revoke Certificates. For purposes of this PDS, CA shall mean the GOV-CA.

"Certificate Policy" or **"CP"** means a set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. For the purpose of this PDS, CP shall mean the GOV-CA CP/CPS document.

"Certification Practice Statement" or **"CPS"** means a document, as revised from time to time, representing a statement of the practices a CA employs in issuing Certificates. For the purpose of this PDS, CPS shall mean the GOV-CA CP/CPS document.

"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 AGCE and governed by the GOV-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 AGCE 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 GOV-CA.

5 Compliance

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

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

6 Certificate Type, Validation Procedures and Usages

The AGCE is established by the Algerian Government to operate CAs that offer certification services to the Algeria government entities. As such the AGCE operates under the National Root CA as follows:

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

  The GOV-CA signing key is permitted only for certifying public keys for Trust Service Providers (TSPs) operating certification services under the Government domain. The certification request of TSP CAs are validated and approved by the AGCE PKI GB. The relevant procedures are detailed in the GOV-CA CP/CPS. The certificate types supported by the GOV-CA are specified in section 7 of the GOV-CA CP/CPS document.

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

  - **Corporate CA**: CA that will issue certificates to natural persons (citizens and government employees) and legal persons (government entities);

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

o **OV TLS CA**: CA that will issue certificates to non-natural entities, such as servers and VPN device certificates.

- **Device Certificates** – Used for device identification and authentication
- **TLS/SSL Certificates** – Used for server authentication and session data encryption
- **VPN Certificates** – Used for device identification and session data encryption for IPSec-based connections
- **OCSP certificates** – used by the AGCE Online Certificate Status Protocol (OCSP) sign OCSP responses for the certificates issued by this CA.

o **Code Signing CA:** CA that will issue code signing certificates to legal persons (government entities).

- **Code signing certificate** – used to sign a source code/software developed by a government entity.
- **OCSP certificates** – used by the AGCE Online Certificate Status Protocol (OCSP) sign OCSP responses for the certificates issued by this CA.

o **SMIME CA:** CA that will issue email protection (SMIME) certificates to natural persons (government employees).

- **Email protection certificate** – used to digitally sign email communications.

  OCSP certificates – used by the AGCE Online Certificate Status Protocol (OCSP) sign OCSP responses for the certificates issued by this CA.

o **Trust Services CA:** CA that will issue both AGCE Timestamping and Verification Service

- **Certificates Issued for Time stamping Authority (TSA)** – Certificates for signing timestamps issued by the AGCE Timestamping Authority service.

- **Verification Response Signing Certificates** – certificate for signing the signature verification response returned from a signature verification service.
- **OCSP certificates** – used by the AGCE Online Certificate Status Protocol (OCSP) sign OCSP responses for the certificates issued by this CA.

7 Obligations

It is the responsibility of the AGCE 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 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 CA operations at all times;
- Provide certificate status validation mechanisms, such as CRLs and OCSP services as applicable; and
- Conduct annual compliance audits and assessments as described in the following documents
    - GOV-CA CP/CPS,
    - AGCE CPS for Devices
    - AGCE CPS for legal and Natural Persons

8 Certificate Status Checking Obligations of Relying Parties

If a Relying Party is to reasonably rely upon a certificate issued by the AGCE 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

AGCE is responsible for the execution of its services as specified in its CPS documents for the Use of AGCE CAs.

AGCE is not liable for:

- the secrecy of the Private Keys of Subscriber
- any misuse of the Subscriber' SubCA 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, AGCE 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 AGCE, 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

AGCE agreements and CPSs can be found at (https://ca.pki.agce.dz/repository).

11 Privacy Policy

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

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

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

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

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

All communications channels with AGCE shall preserve the privacy and confidentiality of any

exchanged private information.

12 Refund Policy

No refunds are applicable for any fees charged by AGCE.

13 Applicable Law and Dispute Resolution

The AGCE acts in accordance with current legislation in the applicable laws of the people's democratic republic of Algeria. In particular:

- law 15-04 fixing "*les règles générales relatives à la signature et à la certification électroniques*".
- Decret executif N°16-134
- Decret executif N°16-135

All disputes associated with the provisions of this document and the AGCE CAs services, shall be first addressed by the PKI GB. If mediation by the PKI GB is not successful, then the dispute will be escalated to the PMA and eventually adjudicated by the relevant courts of Algeria.

14 CA and Repository Licenses, Trust Marks, and Audit

AGCE ensures that its CAs and related services are subject to regular internal audits. These audits are planned and executed, at a minimum, once 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 AGCE and apply for the certification services offered through AGCE CAs.