PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

GOVERNMENT ELECTRONIC CERTIFICATION AUTHORITY

AGCE PKI

Subscriber Agreement for Natural Person Certificates

Version 2.1

Document management

Information

Group of document	AGCE PKI
Title	Subscriber Agreement for Natural Person Certificates
Project reference	Algeria National PKI
Annex	n.a.

Version control

Version	Date	Description / Status	Responsible
V1.0	15/10/2020	Initial released version	AGCE
V2.0	24/7/2023	Updated version to conform to latest policy documents	AGCE
V2.1	08/10/2024	• Updated version to conform to latest policy documents • Updates following AGCE decision to terminate Code Signing and SMIME services.	AGCE

Contents

1. 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 Agreement, CA shall mean the AGCE Issuing CAs.

"Certificate Policy" or **"CP"** means a document, as revised from time to time, representing the set of rules that indicates the applicability of a Certificate issued by AGCE to a subscriber.

"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. In the context of this agreement, the CPS shall mean the AGCE CPS for Legal and Natural, all AGCE CPSs being published at AGCE's public repository at the address at https://ca.pki.agce.dz/repository.

"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).

"Local Registration Authority" or "LRA" refers to the organization entering in an agreement with AGCE through which AGCE delegates important aspects of certificate lifecycle management of the organization user base. Refer to the **RA** definition.

"Public Key Infrastructure" or **"PKI"** means 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. In the context of this agreement, PKI shall refer to the PKI operated by AGCE to enable the deployment and use of Certificates issued by the AGCE Corporate.

"Registration Authority" or **"RA"** means a Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA. In the context of this Agreement, the RA term refers to

AGCE internal RA that is responsible for exposing and fulfilling the certifications services from AGCE CAs.

"Repository" A trustworthy system for storing and retrieving certificates or other information relevant to certificates. AGCE public repository is accessible at the address at https://ca.pki.agce.dz/repository.

"Services" mean, collectively, the services offered by AGCE to Subscribers in delivering digital certificate issuing and revocation services together with the related supporting functions.

"Subscriber" means the natural person to whom a Certificate is issued and who is legally bound by this Subscriber Agreement.

2. Services provided by AGCE

The AGCE operates the Issuing CAs that are dedicated to the issuance of certificates for the natural persons. The Legal and Natural Person CPS describes the AGCE practices in operating the Issuing CAs.

The AGCE exposes the Issuing CAs certificate management functions through a web-based service referred to as the AGCE Web RA portal. Subscribers are enrolled to the AGCE Web RA portal which will provide digital certificate management.

The AGCE exposes the following core functionalities through the Web RA portal:

1. Ability to enroll users.
2. Ability to submit certificate requests.
3. Ability to submit certificate revocation for the users.
4. Ability to manage remote signing certificates and integrations.

The AGCE ensures the availability of the Web RA portal as a 24 × 7 service. The Web RA portal processes instantly certificate management requests triggered by its users and administrators.

The AGCE ensures that certificate validation services are exposed to relying parties through Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP).

The AGCE ensures that the Issuing CA CPS and other public information (including this agreement) are published in a public repository that is available 24 × 7 and accessible at https://ca.pki.agce.dz/repository.

2.1. Contact information

AGCE can be contacted at the following address:

Autorité Gouvernementale de Certification Electronique.
Cyber Park Sidi Abdellah, Bt D,
Rahmania, Zeralda, Alger.

Tel: + 213 (0) 23 202 327

General enquiry email: Certification.Info@agce.dz

Certificate Problem reporting: Certification.Problem@agce.dz

3. Subscriber's Obligations

3.1 Certificate requests

The Subscriber accepts the Terms and Conditions of this Subscriber Agreement, the Conditions as declared by the AGCE through its online services and shall adhere to the requirements provided in the corresponding AGCE CPS.

The Subscriber has the right to submit an application for issuing a Certificate using the processes and systems made available by the AGCE as documented in provided manuals. By completing the user enrollment and submitting a certificate request through the Web RA application.

3.2 Data Accuracy and Control

The Subscriber shall provide accurate and complete information when requesting a certificate. The Subscriber shall refrain from submitting to AGCE any material that contains statements that violate any law or the rights of any party.

Regardless of any certificate issued through the Issuing CAs, should any identifying information change, the subscriber shall immediately initiate communication with AGCE or LRA.

3.3 Key Generation and Usage

The Subscriber shall be responsible to ensure that the subscriber or LRA use a FIPS 140-2 level 2 compliant device to generate the subscriber's keys.

The Subscriber and the LRA shall use the AGCE Web RA portal for submitting certificate management requests to the Issuing CAs.

The Subscriber maintains reasonable measures to maintain sole control, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested certificate.

The Subscriber shall use the certificate(s) issued by AGCE CA solely in compliance with the applicable certificate use. Under no circumstances shall a certificate be used for criminal activities such as phishing attacks, fraud, certifying or signing malware.

3.4 Certificate usage

The Subscriber agrees to use the Certificates received from AGCE only for the intended uses as follows:

- **Signing certificate** – used to produce digital signatures on documents and e-transactions.
- **Authentication certificate** – used to authenticate end-users to e-services

The Subscriber shall not use the certificate until it has reviewed and verified the accuracy of the data incorporated into the certificate.

The certificate is deemed accepted if no complaints are raised by the Subscriber to the LRA or the AGCE RA officer within 5 business days from receiving the certificate.

3.5 Notification and revocation

The Subscriber shall promptly cease using the certificate and its associated Private Key, and promptly request AGCE or LRA to revoke the certificate.

The AGCE or LRA will process the revocation request within 24 hours if one or more of the following occur:

1. The AGCE receives a revocation request through the agreed channels from the applicant representative without specifying a CRLreason (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. It was discovered that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The AGCE obtains reasonable evidence that the subscriber's private key, corresponding to the public key certificate, has been compromised (CRLReason #1, keyCompromise);

The AGCE may revoke a certificate within 24 hours and shall revoke a certificate within 5 days if one or more of the following occurs:

1. Obtaining evidence that the certificate no longer complies with the requirements of sections 6.1.5 and 6.1.6 of the Issuing CA CPS (CRLReason #4, superseded);
2. Obtaining evidence that the certificate was misused (CRLReason #9, privilegeWithdrawn);
3. Knowing that a subscriber has violated one or more of its material obligations under the subscriber Agreement (CRLReason #9, privilegeWithdrawn);
4. Made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
5. Discovering that the certificate was issued in a manner not in accordance with the procedures of the CPS and with the Baseline Requirements (CRLReason #4, superseded);
6. Knowing that any of the information contained in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
7. AGCE's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless AGCE has planned to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
8. Revocation is required by the Issuing CA CPS for a reason that is not otherwise required to be specified by this section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
9. Discovering that there is a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise);
10. Determination that the certificate was issued to an entity other than the one named as the subject of the certificate (CRLReason #1, keyCompromise);
11. A third party provides information that leads the CA to believe that the certificate is compromised or is being used for suspect code (CRLReason #1, keyCompromise);

12. The entity or the subscriber has been declared legally incompetent (CRLReason #9, privilegeWithdrawn).

3.6 Permission to Publish Information

The Subscriber allows AGCE to publish the serial number of the Subscriber's certificate in connection with dissemination of CRL's and OCSP services.

4. Disclaimer of Warranty

AGCE is responsible for the execution of its services as specified in its Certification Practice Statement (CPS).

AGCE is not liable for:

- the secrecy of the Private Keys of Subscriber
- any misuse of the Subscriber Certificates 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 laws of 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

5. Privacy

AGCE and LRA observe personal data privacy rules and privacy rules as specified in AGCE CPS for the Issuing CAs.

Only limited trusted personnel from AGCE and LRA shall be permitted to access subscriber information for the purpose of certificate lifecycle management.

AGCE and LRA 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.

AGCE and LRA 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 and LRA shall preserve the privacy and confidentiality of any

exchanged subscriber private information.

6. Term and Termination

This agreement shall terminate at the earliest of:

- The expiry date of the certificate issued to the subscriber,
- The revocation of the certificate issued to the subscriber
- The affiliation between the subscriber and the LRA ends

6.1 Effect of termination

Upon termination of this Subscriber Agreement for any reason, AGCE and LRA may revoke the Subscriber's certificate in accordance with AGCE CPS.

7. Miscellaneous Provisions

7.1 Governing Laws

The laws of the people's democratic republic of Algeria shall govern the enforceability, construction, interpretation, and validity of the present Agreement.

7.2 Entire Agreement

This Agreement constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties.

7.3 Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto.