PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

GOVERNMENT ELECTRONIC CERTIFICATION AUTHORITY

AGCE PKI

Subscriber Agreement for Legal Person Certificates

Version 2.0

July 2023

Document management

Information

Group of document	**AGCE PKI**
Title	**Subscriber Agreement for Legal 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

Table of 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 Person and the AGCE CPS for Devices, depending on the type of the requested certificate, 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).

"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.

"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. 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 legal Entity to whom a Certificate is issued and who is legally bound by this Subscriber Agreement.

"Subject" means the device, system, unit, or legal Entity identified in a Certificate as the Subject. In the context of this agreement, Subject populate the certificates issued by AGCE Issuing CAs depending on the type of certificates.

2. Services provided by AGCE

Without prejudice to Section 4 of this Subscriber Agreement, AGCE shall provide its services in accordance with the Certification Practice Statement (CPS) documents for the respective AGCE CAs. The AGCE shall provide the following services to Subscribers in relation to the fulfillment of its services:

- Certificate enrolment, certificate requests and revocation requests through AGCE RA function;
- Certificate issuance and revocation services;
- Certificate Revocation Lists (CRL) issuance and publishing on AGCE public repository;
- Online certificate Status Protocol (OCSP) services and responses;
- Publishing relevant agreements, policies and practice statements on AGCE public repository;
- Helpdesk service to respond to certificate problem requests.

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 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 AGCE as documented in AGCE Subscriber Manual for High Trust Certificates.

3.2. Exclusive control

For TLS server certificates, the Subscriber acknowledges and asserts that they have exclusive control of the domain(s) or IP Address listed in the SubjectAltName(s) for which they are applying for the SSL/TLS certificate.

Regardless of the certificate type, should the subscriber cease to exclusively own the domain, e-mail address or other identifying information, the subscriber shall immediately inform AGCE who will promptly revoke the certificate in accordance with the corresponding AGCE CPS.

3.3. Data Accuracy

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. This includes no misleading information within the Subject:organizationName and the Subject:organizationalUnitName attributes.

3.4. Key Generation and Usage

The Subscriber shall be responsible to ensure that trustworthy systems and methods shall be used in order to generate public-private key pairs, moreover key lengths and algorithms must be used which is recognized as being fit for the requested certificate as per AGCE applicable CPS.

The Subscriber shall ensure that the Public Key submitted to AGCE corresponds to the Private Key used.

The Subscriber shall exercise appropriate and reasonable care to avoid unauthorized use of its Private Key.

For code signing certificates, the private key should be generated in a FIPS 140-2 level 3 or equivalent hardware security device.

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 AGCE CA CPS and this subscriber agreement. Under no circumstances shall a certificate be used for criminal activities such as phishing attacks, fraud, certifying or signing malware.

3.5. Certificate acceptance

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 AGCE within 10 business days from receiving the certificate.

3.6. Certificate usage

The Subscriber undertakes to use the Certificates received from AGCE only for the intended uses as specified by the corresponding AGCE CPS.

3.7. Notification and revocation

The Subscriber undertakes to promptly cease using the certificate and its associated Private Key, and promptly requests AGCE to revoke the certificate.

The AGCE revokes a certificate within 24 hours if one or more of the following occurs:

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);
4. The AGCE obtains evidence that the validation of domain authorization or control for any FullyQualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

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 (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. In relation to code signing, the Subscriber has signed code containing malicious code or serious vulnerabilities (CRLReason #9, privilegeWithdrawn);
5. Coming across any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
6. Knowing that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
7. Made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
8. Discovering that the certificate was issued in a manner not in accordance with the procedures of this CPS and with the Baseline Requirements (CRLReason #4, superseded);
9. Knowing that any of the information contained in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
10. 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);
11. Revocation is required by this 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);
12. 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);

13. Determination that the certificate was issued to an entity other than the one named as the subject of the certificate (CRLReason #1, keyCompromise);
14. 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);
15. The entity or the subscriber has been declared legally incompetent (CRLReason #9, privilegeWithdrawn).

3.8. 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) for the Use of TLS server certificates.

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

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.

6. Term and Termination

This agreement shall terminate at the earliest of:

- The expiry date of any certificate issued to the subscriber;
- Failure by the Subscriber to perform any of its material obligations under this Subscriber Agreement.

6.1. Effect of termination

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