ECONOMIC AUTHORITY OF ELECTRONIC CERTIFICATION

AECE PKI

Subscriber Agreement for Subordinate CA

Version 1.0

Document management

Information

Group of document	AECE
Title	Subscriber Agreement for Subordinate CA
Project reference	Algeria National PKI
Annex	n.a.

Version control

Version	Date	Description / Status	Responsible
V 1.0	15/01/2020	Initial document preparation	AECE

Table of contents

1 Definitions and Acronyms

"AECE" means Autorité Economique de Certification Électronique.

"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 Commercial CA operated by AECE (COM-CA).

"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 AECE to a subscriber Subordinate CA.

"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 AECE COM-CA CP/CPS being published at AECE's public repository at the address at https://pki.aece.dz/repository.

"CP/CPS" means CPS in the context of this agreement. Refer to CPS definition.

"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).

"PKI GB" means PKI Governance board. In the context of this agreement and as per the Algeria PKI governance model, the PKI GB represents the management structure of AECE.

"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. In the context of this Agreement, the RA term refers to the RA function of the AECE.

"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. AECE public repository is accessible at the address at https://pki.aece.dz/repository.

"Services" mean, collectively, the services offered by AECE 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.

"Subscriber Agreement" means an agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties. This present document is the Subscriber Agreement to be signed by AECE Subscribers.

2 Services Provided by AECE

Without prejudice to Section 4 of this Subscriber Agreement, AECE shall provide its services in accordance with the COM-CA CP/CPS. The AECE shall provide the following services to Subscribers in relation to the fulfillment of its services:

- 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

2.1 Contact Information

AECE can be contacted 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

General enquiry email: info@aece.dz

Certificate Problem reporting: reports@aece.dz

3 AECE's Obligations

AECE shall act as the Certification Authority for the Subscriber's Subordinate CA Certificate and perform its obligations as specified in this Agreement and the COM-CA CP/CPS.

AECE will sign the Subscriber's Subordinate CA CSR during a Key ceremony where the Subscriber's Subordinate CA representatives are present. AECE shall offer the additional services as listed under section 2 of this agreement.

4 Subscriber's Obligations

4.1 Certificate Request

The Subscriber accepts the Terms and Conditions of this Subscriber Agreement and shall adhere to the requirements provided in the COM-CA CPS.

The Subscriber has the right to submit an application for issuing a Certificate using the processes agreed with AECE and as specified in the COM-CA CPS.

4.2 Data Accuracy

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

4.3 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 the COM-CA CP/CPS,
- The Subscriber shall ensure that the Public Key submitted to AECE corresponds to the Private Key used,
- The Subscriber shall exercise appropriate and reasonable care to avoid unauthorized use of its Private Key.
- 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 the COM-CA solely in compliance with the COM-CA CP/CPS and this subscriber agreement. Under no circumstances shall a certificate be used for criminal activities.

4.4 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 AECE within 10 business days from receiving the certificate.

4.5 Certificate usage

The Subscriber undertakes to use the Certificates received from AECE only for the intended uses as specified by the COM-CA CPS.

4.6 Notification and revocation

The Subscriber undertakes to promptly cease using the certificate and its associated Private Key, and promptly request AECE to revoke the certificate, in the event that:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key of the certificate's “Subject”,
- The Subscriber indicates that the original certificate Signing Request (CSR) was not authorized and does not retroactively grant authorization,
- The Subscriber has breached a material obligation of the COM-CA CP/CPS,
- The Subscriber requests in writing that AECE revoke the certificate,
- The performance of a person's obligations under the COM-CA CP/CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised,
- There has been a modification of the information regarding the “Subject” of the certificate,
- This Subscriber Agreement has been terminated,
- The information within the certificate, other than non - verified “Subscriber Information” contained in the “O” field, is incorrect or has changed,

- Termination of use of the certificate.

4.7 Permission to Publish Information

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

5 Disclaimer of Warranty

AECE is responsible for the execution of its services as specified in the COM-CA CP/CPS for the Use of Subscriber's Subordinate CA Certificates.

AECE is not liable for:

- the secrecy of the Private Keys of Subscriber
- any misuse of the Subscriber' Subordinate 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

6 Privacy

AECE observes personal data privacy rules and privacy rules as specified in the COM-CA CP/CPS.

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.

7 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.

7.1 Effect of termination

Upon termination of this Subscriber Agreement for any reason, AECE may revoke the Subscriber's certificate in accordance with COM-CA CP/CPS.

8 Miscellaneous Provisions

8.1 Governing Laws

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

8.2 Entire Agreement

This Agreement constitutes the entire agreement between the parties in relation to the execution of the related PKI services and supersedes all prior understandings, oral or written, between the parties.

8.3 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.

Official Representative Name: _____

☐ I hereby acknowledge that I have read, understand, and agree to the terms and conditions of this Subscriber agreement

_____ _____

Official Representative Signature Stamp