

**APPLICATION FORM & AGREEMENT FOR QUALIFIED CERTIFICATE
FOR ELECTRONIC SEAL
(LEGAL PERSON)
ACCORDING TO EU PAYMENT SERVICES DIRECTIVE (PSD2)**

Fill in the fields in capital letters exactly as given in your identification documents (ID or passport).

- (1) Fields are filled in by ADACOM S.A.
- (2) Fields are included in the Certificate data.
- (3) Fields with data non verified by ADACOM.
- (4) Email address provided will be used for receiving the csr of Certificate.
- (5) Please include the Country of Payment Service Provider.
- (6) Please include the Company Name or Distinctive Title as in the Articles of Association or in the Commercial Registry.
- (7) The authorization number or registration number issued by the local National Competent Authority, which supervises the financial services of the Legal Person
- (8) The name of the local National Competent Authority which supervises the financial services of the Legal Person
- (9) Account servicing (PSP_AS) or payment initiation (PSP_PI) or account information (PSP_AI) or issuing of card-based payment instruments (PSP_IC)

Date: _____ (1)A/A: _____

APPLICANTS DATA

Legal Person's name: (2) (6) _____

Type of entity : _____

Tax Identity Number (TIN) / National Trade Registry (NTR): _____

PSP Authorization Number: (2) (7) _____

National Competent Authority Name: (2) (8) _____

National Competent Authority ID: (2) _____

Country: (2) (5) _____

Address and Post Code: (3) _____

Telephone Number (fixed line): (3) _____

Telephone Number (mobile): (3) _____

E-mail address: (4) _____

PSP Role(s) (2) (9) : Account servicing(PSP_AS): Payment initiation(PSP_PI)

 Account Information (PSP_AI) Issuing of card-based payment instruments(PSP_IC)

Legal person's representative

First Name: _____

Last Name: _____

Title: _____

National ID or Passport Number: _____

QSCD Qualified Signature Creation Device	YES <input type="checkbox"/>	NO <input type="checkbox"/>
--	-------------------------------------	------------------------------------

This Application-Agreement is subject to the following terms, which must be accepted by the Subscriber signing at the end of the document:

1. The identity verification of the Subscriber shall be effected in one of the following ways:
 - by sending via email to ira@adacom.com the following documents, **digitally signed** by Subscriber's Legal Representative of PSP with a Qualified Electronic Signature under eIDAS Regulation:
 1. The Application Form for Qualified Certificate for electronic seal (QeSeal) filled in all of its parts and digitally signed by the Legal Representative of the PSP with a Qualified Electronic Signature under eIDAS Regulation.
 2. A copy of National ID or Passport of the Legal representative of the PSP digitally signed with a Qualified electronic signature under eIDAS Regulation.
 3. All the necessary documentation containing PSD2 specific attributes:
 - Authorization Number or other recognized identifier
 - The role of the PSP (PSP_AS, PSP_PI, PSP_AI, PSP_IC)
 - NCA Name
 - NCA ID (unique identifier)
 4. Proof of full name and Legal status of the Legal Person based on certified copies of Organizational documents evidencing the official registration, the existence and operation of the Legal Person.

Additional verification will be performed by ADACOM consisting of:

- Validation of the PSP authorization number or any other registration number provided against NCA/EBA registry
- Validation of the role of PSP (PSP_AS, PSP_PI, PSP_AI, PSP_IC) against the NCA/EBA registry.

**APPLICATION FORM & AGREEMENT FOR QUALIFIED CERTIFICATE
FOR ELECTRONIC SEAL
(LEGAL PERSON)
ACCORDING TO EU PAYMENT SERVICES DIRECTIVE (PSD2)**

2. This Application Form constitutes the agreement between the Subscriber and ADACOM and will become effective on the date of signature this Application Form. By submitting this Application, the Subscriber requests that ADACOM issue a Qualified Certificate for Electronic Seal to the Subscriber. The Subscriber can complete the enrollment process within one month from the date of submission of this Application Form. ADACOM's Qualified Trust Services are governed by ADACOM's Certification Practice Statement (CPS) as amended from time to time, as well as ADACOM's General Terms and Conditions for Use of Qualified Trust Services, which are incorporated into this Agreement and are published on ADACOM's repository at <https://pki.adacom.com/repository>

3. Subscriber may require the non-publication of the certificate to ADACOM's Public Directory during the electronic enrollment that follows the submission and acceptance of the present Application;

4. Subscriber warrants and represents that all information provided for the issuance of the Certificate is complete, accurate and correct and that the Subscriber is legally eligible to submit this Application Form; ADACOM confirms that the information to be held in the certificate is correct.

5. If the Subscriber chooses to use a Qualified Signature Creation Device (QSCD), he agrees to use a secure cryptographic device, which will be provided by ADACOM, and the Subscriber is solely responsible for its use. Subscriber shall treat the QSCD as any object containing private data and shall not lend the QSCD or disclose its PIN to anyone.

6. Upon facing a problem or upon having suspicions that:

i) Subscriber's private key has been lost, stolen, potentially compromised; or

ii) Control over the Subscriber 's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or

iii) Inaccuracy or changes to the certificate content.

Contact ADACOM Customer Support at once at +30 210 95 77 255.

7. Subscriber may request revocation of the Certificate via email at psd2@adacom.com or via phone at +30 210 9577255.

8. Subscriber is solely responsible for the payment of any fees, costs and indemnities associated with the Certificate's issuance and the use of the Certificate.

NOTICE REGARDING PERSONAL DATA PROCESSING

CATEGORIES OF PERSONAL DATA

ADACOM keeps a record of information used during the registration, device provision and any subsequent revocation, the identity information and any other attributes placed in the certificate.

PURPOSE OF PROCESSING

ADACOM process personal data in order to issue certificates and provide consultancy services to the Subscriber.

RETENTION PERIOD

The record of certificates and the related documents is kept for at least 7 years or as required in compliance with applicable laws. The retention period is calculated from the expiration or revocation date of the certificate.

TRANSFERRING INFORMATION TO THIRD PARTIES

In case ADACOM terminates its services, the aforementioned record will be transferred to another Qualified Trust Service Provider.

The Applicant-Subscriber

(1)Authenticated by RA or LRA

Name/ Surname:

Title:

Signature:

Name/ Surname:

Title:

Signature:
