ADACOM

QUALIFIED TRUST SERVICES

User guide for remote qualified certificates in remote QSCD

1. Introduction

This document is a digital certificate enrolment guide.

You may find the information required, as well as a step-by-step guide for obtaining a Remote Qualified Certificate for electronic signature.

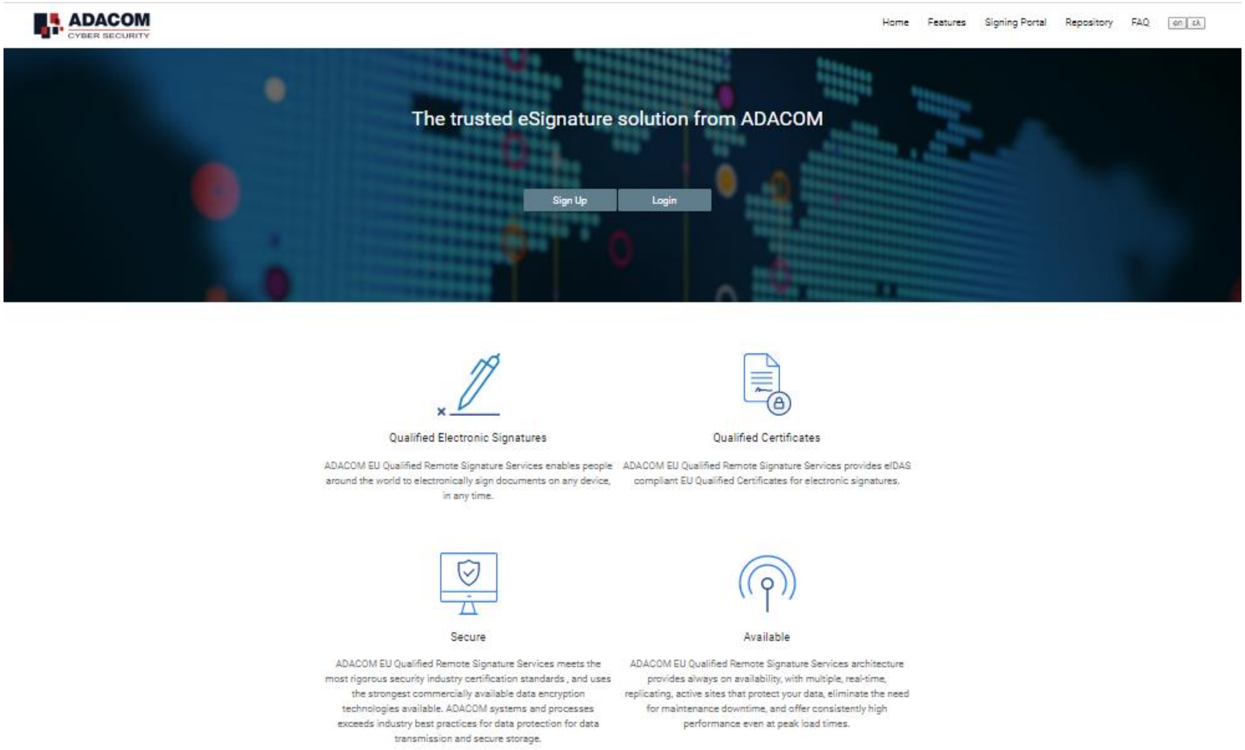
2. User Portal Registration

The first step is to create an account to the ADACOM QTSP Services Portal, as described below

2.1 Registration Procedure

a) To register, using any browser visit the following url and choose “Sign Up”

- For real certificates https://aqs-portal.adacom.com
- For test environment https://aqs-portal-test.adacom.com



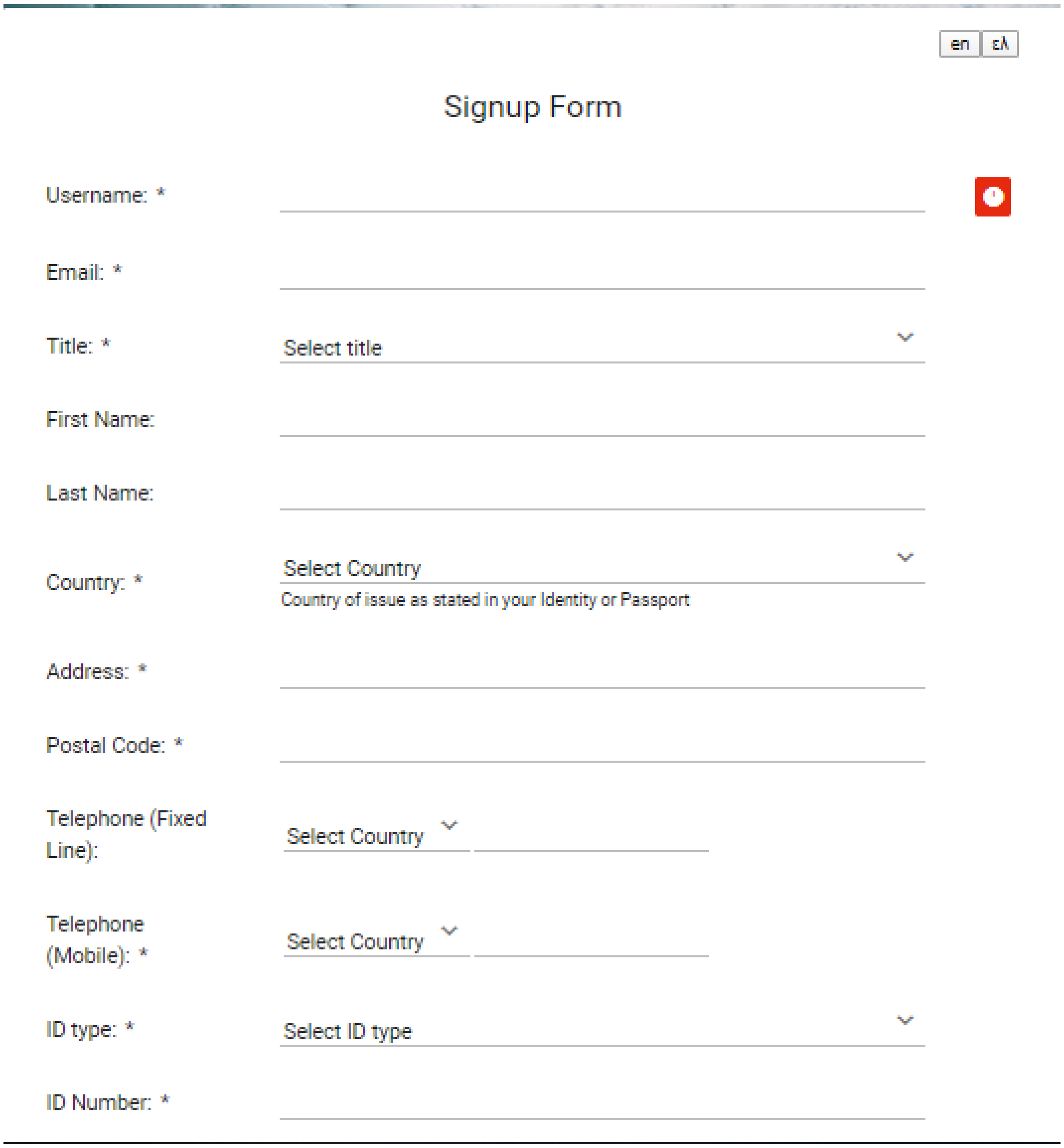
ADACOM EU Qualified Remote Signature Services enables people around the world to electronically sign documents on any device, in any time.

ADACOM EU Qualified Remote Signature Services provides eIDAS compliant EU Qualified Certificates for electronic signatures.

ADACOM EU Qualified Remote Signature Services meets the most rigorous security industry certification standards , and uses the strongest commercially available data encryption technologies available. ADACOM systems and processes exceeds industry best practices for data protection for data transmission and secure storage.

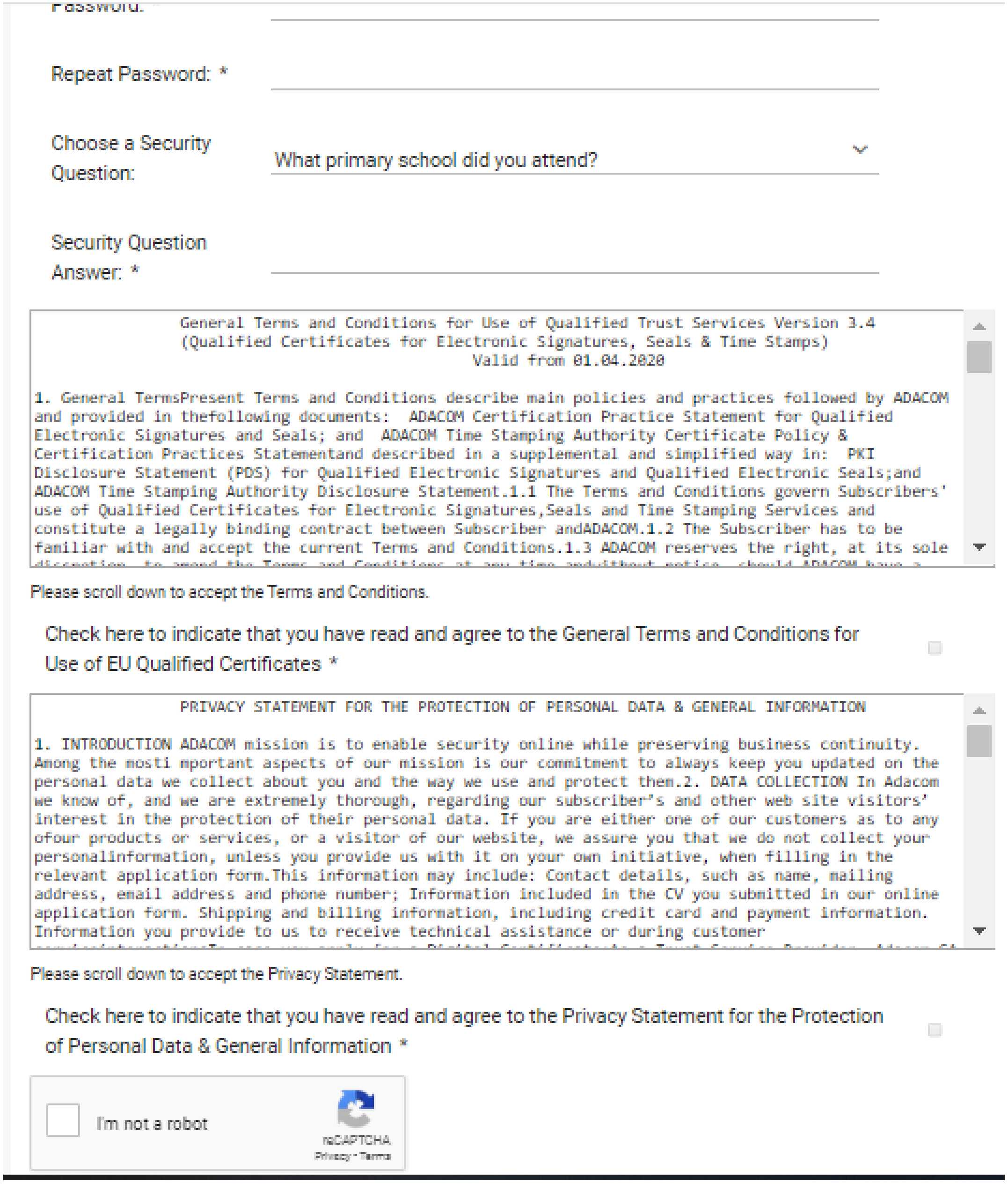
ADACOM EU Qualified Remote Signature Services architecture provides always on availability, with multiple, real-time, replicating, active sites that protect your data, eliminate the need for maintenance downtime, and offer consistently high performance even at peak load times.

b) Fill in all required information and choose “Submit”



Signup Form

Username: *		
Email: *		
Title: *	Select title	
First Name:		
Last Name:		
Country: *	Select Country Country of issue as stated in your Identity or Passport	
Address: *		
Postal Code: *		
Telephone (Fixed Line):	Select Country	
Telephone (Mobile): *	Select Country	
ID type: *	Select ID type	
ID Number: *		



Password: *

Repeat Password: *

Choose a Security Question: What primary school did you attend?

Security Question Answer: *

General Terms and Conditions for Use of Qualified Trust Services Version 3.4
(Qualified Certificates for Electronic Signatures, Seals & Time Stamps)
Valid from 01.04.2020

1. General TermsPresent Terms and Conditions describe main policies and practices followed by ADACOM and provided in thefollowing documents: ADACOM Certification Practice Statement for Qualified Electronic Signatures and Seals; and ADACOM Time Stamping Authority Certificate Policy & Certification Practices Statementand described in a supplemental and simplified way in: PKI Disclosure Statement (PDS) for Qualified Electronic Signatures and Qualified Electronic Seals;and ADACOM Time Stamping Authority Disclosure Statement.1.1 The Terms and Conditions govern Subscribers' use of Qualified Certificates for Electronic Signatures,Seals and Time Stamping Services and constitute a legally binding contract between Subscriber andADACOM.1.2 The Subscriber has to be familiar with and accept the current Terms and Conditions.1.3 ADACOM reserves the right, at its sole

Please scroll down to accept the Terms and Conditions.

Check here to indicate that you have read and agree to the General Terms and Conditions for Use of EU Qualified Certificates * □

PRIVACY STATEMENT FOR THE PROTECTION OF PERSONAL DATA & GENERAL INFORMATION

1. INTRODUCTION ADACOM mission is to enable security online while preserving business continuity. Among the mosti mportant aspects of our mission is our commitment to always keep you updated on the personal data we collect about you and the way we use and protect them.2. DATA COLLECTION In Adacom we know of, and we are extremely thorough, regarding our subscriber's and other web site visitors' interest in the protection of their personal data. If you are either one of our customers as to any ofour products or services, or a visitor of our website, we assure you that we do not collect your personalinformation, unless you provide us with it on your own initiative, when filling in the relevant application form.This information may include: Contact details, such as name, mailing address, email address and phone number; Information included in the CV you submitted in our online application form. Shipping and billing information, including credit card and payment information. Information you provide to us to receive technical assistance or during customer

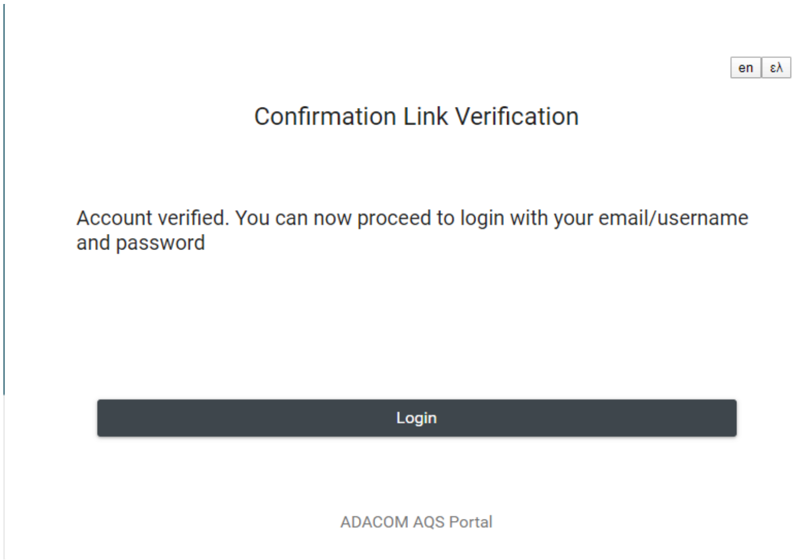
Please scroll down to accept the Privacy Statement.

Check here to indicate that you have read and agree to the Privacy Statement for the Protection of Personal Data & General Information * □

The above information should be valid, as this data will be used for your certificate application.

c) After you press "submit", a confirmation email will be sent to the provided email address

d) Click the link in the email received, to confirm your registration



Confirmation Link Verification

Account verified. You can now proceed to login with your email/username and password

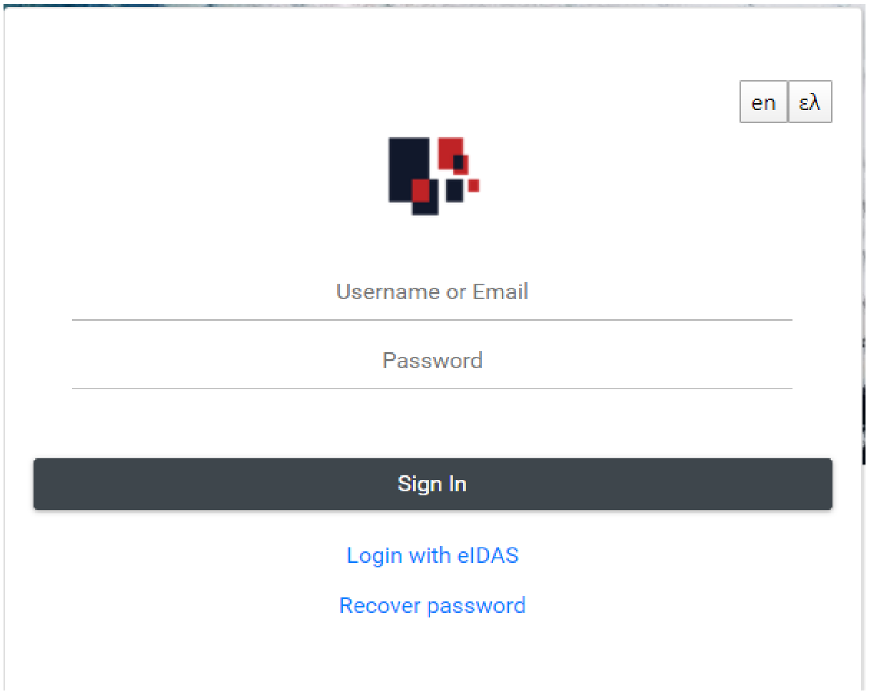
Your registration is now complete. You may login to the ADACOM QTSP Services Portal at any time.

2.2 Login Procedure

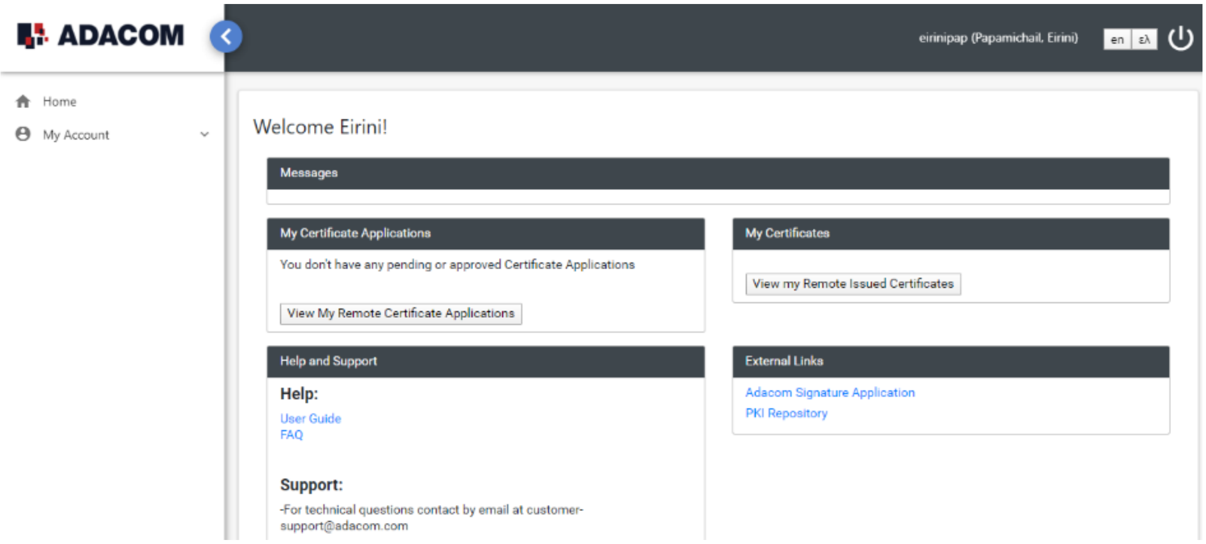
a) Using any browser visit the ADACOM QTSP Services Portal at the below url:

- For real certificates https://aqs-portal.adacom.com
- For test environment https://aqs-portal-test.adacom.com

b) Choose “Login”



c) Provide your **username** and **password** that you have provided during the previous registration form and press **“Sign in”**


ADACOM
eirinipap (Papamichail, Eirini)
en
ελ
Home
My Account

Welcome Eirini!

Messages

My Certificate Applications

You don't have any pending or approved Certificate Applications

View My Remote Certificate Applications

My Certificates

View my Remote Issued Certificates

Help and Support

Help:

User Guide
FAQ

Support:

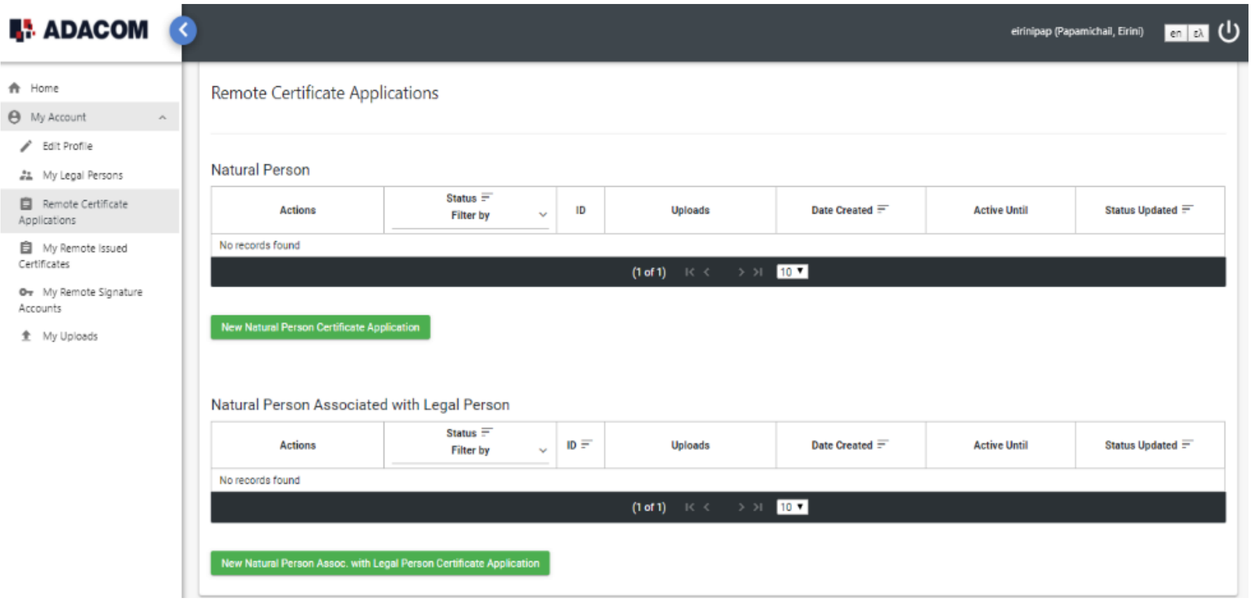
-For technical questions contact by email at customer-support@adacom.com

External Links

Adacom Signature Application
PKI Repository

3. Certificate Application Procedure

a) To create a Certificate Application, select **“Remote Certificate Applications”**


ADACOM
eirinipap (Papamichail, Eirini)
en
ελ
Home
My Account
Edit Profile
My Legal Persons
Remote Certificate Applications
My Remote Issued Certificates
My Remote Signature Accounts
My Uploads

Remote Certificate Applications

Natural Person

Actions	Status Filter by	ID	Uploads	Date Created	Active Until	Status Updated
No records found						

(1 of 1)
10
New Natural Person Certificate Application

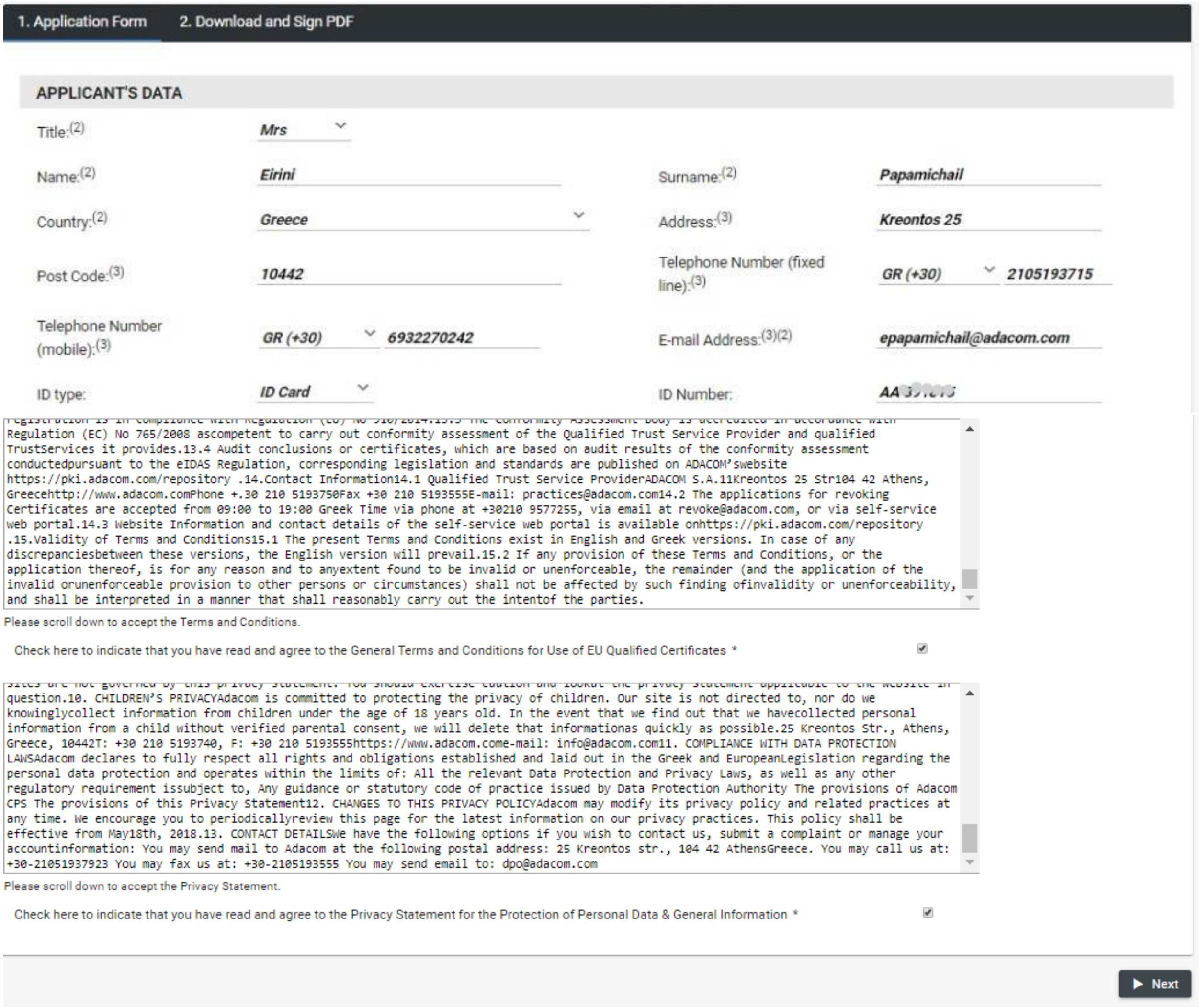
Natural Person Associated with Legal Person

Actions	Status Filter by	ID	Uploads	Date Created	Active Until	Status Updated
No records found						

(1 of 1)
10
New Natural Person Assoc. with Legal Person Certificate Application

b) Select the type of certificate you want to request:

- **New Natural Person Certificate Application**
- **New Natural Person Assoc. with Legal Person Certificate Application**



APPLICANT'S DATA

Title:(2)	Mrs		
Name:(2)	Eirini	Surname:(2)	Papamichail
Country:(2)	Greece	Address:(3)	Kreontos 25
Post Code:(3)	10442	Telephone Number (fixed line):(3)	GR (+30) 2105193715
Telephone Number (mobile):(3)	GR (+30) 6932270242	E-mail Address:(3)(2)	epapamichail@adacom.com
ID type:	ID Card	ID Number:	AA [redacted]

Regulation (EC) No 765/2008 ascompetent to carry out conformity assessment of the Qualified Trust Service Provider and qualified TrustServices it provides.13.4 Audit conclusions or certificates, which are based on audit results of the conformity assessment conductedpursuant to the eIDAS Regulation, corresponding legislation and standards are published on ADACOM'swebsite https://pki.adacom.com/repository .14.Contact Information14.1 Qualified Trust Service ProviderADACOM S.A.11Kreontos 25 Str104 42 Athens, Greecehttp://www.adacom.comPhone +.30 210 5193750Fax +30 210 5193555E-mail: practices@adacom.com14.2 The applications for revoking Certificates are accepted from 09:00 to 19:00 Greek Time via phone at +30210 9577255, via email at revoke@adacom.com, or via self-service web portal.14.3 Website Information and contact details of the self-service web portal is available onhttps://pki.adacom.com/repository .15.Validity of Terms and Conditions15.1 The present Terms and Conditions exist in English and Greek versions. In case of any discrepanciesbetween these versions, the English version will prevail.15.2 If any provision of these Terms and Conditions, or the application thereof, is for any reason and to anyextent found to be invalid or unenforceable, the remainder (and the application of the invalid orunenforceable provision to other persons or circumstances) shall not be affected by such finding ofinvalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intentof the parties.

Please scroll down to accept the Terms and Conditions.

Check here to indicate that you have read and agree to the General Terms and Conditions for Use of EU Qualified Certificates * ☑

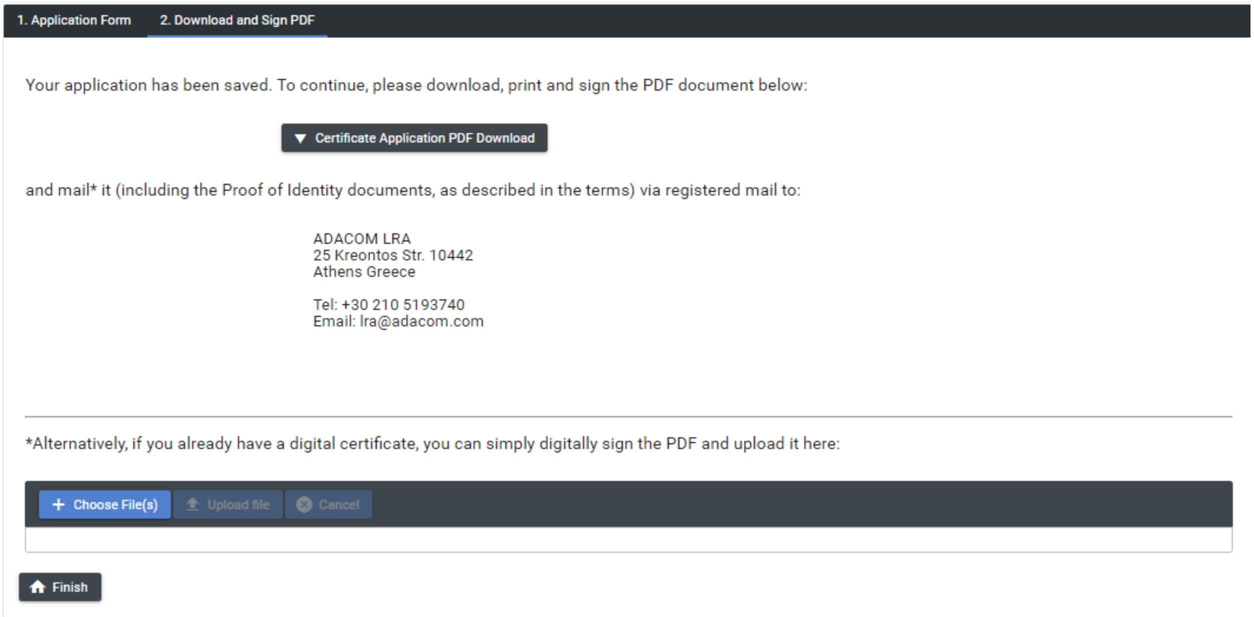
question.10. CHILDREN'S PRIVACYAdacom is committed to protecting the privacy of children. Our site is not directed to, nor do we knowinglycollect information from children under the age of 18 years old. In the event that we find out that we havecollected personal information from a child without verified parental consent, we will delete that informationas quickly as possible.25 Kreontos Str., Athens, Greece, 10442T: +30 210 5193740, F: +30 210 5193555https://www.adacom.come-mail: info@adacom.com11. COMPLIANCE WITH DATA PROTECTION LAWSAdacom declares to fully respect all rights and obligations established and laid out in the Greek and EuropeanLegislation regarding the personal data protection and operates within the limits of: All the relevant Data Protection and Privacy Laws, as well as any other regulatory requirement issubject to, Any guidance or statutory code of practice issued by Data Protection Authority The provisions of Adacom CPS The provisions of this Privacy Statement12. CHANGES TO THIS PRIVACY POLICYAdacom may modify its privacy policy and related practices at any time. We encourage you to periodicallyreview this page for the latest information on our privacy practices. This policy shall be effective from May18th, 2018.13. CONTACT DETAILSWe have the following options if you wish to contact us, submit a complaint or manage your accountinformation: You may send mail to Adacom at the following postal address: 25 Kreontos str., 104 42 AthensGreece. You may call us at: +30-21051937923 You may fax us at: +30-2105193555 You may send email to: dpo@adacom.com

Please scroll down to accept the Privacy Statement.

Check here to indicate that you have read and agree to the Privacy Statement for the Protection of Personal Data & General Information * ☑

c) Check the validity of your information. You may edit any data necessary. Your First and Last Name **must match your ID or Passport,** otherwise your application should be rejected.

d) Scroll down the terms and conditions and then click the checkbox in order to them as well as the privacy policy and then click **"Next".**



Your application has been saved. To continue, please download, print and sign the PDF document below:

and mail* it (including the Proof of Identity documents, as described in the terms) via registered mail to:

ADACOM LRA
25 Kreontos Str. 10442
Athens Greece

Tel: +30 210 5193740
Email: lra@adacom.com

*Alternatively, if you already have a digital certificate, you can simply digitally sign the PDF and upload it here:

e) Click "**Certificate Application PDF Download**" to download the certificate application you created in pdf format

***Note*: If you have already received your application and completed it, skip this step.**

f) Open the PDF file with Acrobat Reader DC and:

- In case you do not have a valid Qualified Certificate for electronic signatures:
  - you will have to print the application form and sign it
  - with the Proof of your Identity documents you have to send the notarized copies by your physical presence or via mail (post) to the following address:

    ADACOM LRA
    25 Kreontos Str. 10442 Athens, Greece
    Tel +30 210 5193740
    Email : lra@adacom.com
- In case you do have a valid Qualified Certificate for electronic signatures:
  - then you may sign the application form digitally.
  - Afterwards, click the **"+ Choose"** button and upload the signed document.
  - Repeat this procedure for your Proof of Identity documents.
  - Click the **"Upload File"**

Note: You can repeat the uploading as many times as you like.

- Select My Account > My Certificate Applications
- Choose the ID of your application
- Choose **"Next"** and you will see the page where you can upload documents.

g) Choose **"Finish"**

As soon as your Certificate Application and Proof of Identity documents will be reviewed successfully by the ADACOM Registration Authority, you will be notified via email.

4. Approval of the issuance of the Qualified Certificate

There will be a process of confirming the details of the application and identifying the user data from ADACOM, and then you will receive an email update on whether your application was approved or rejected.

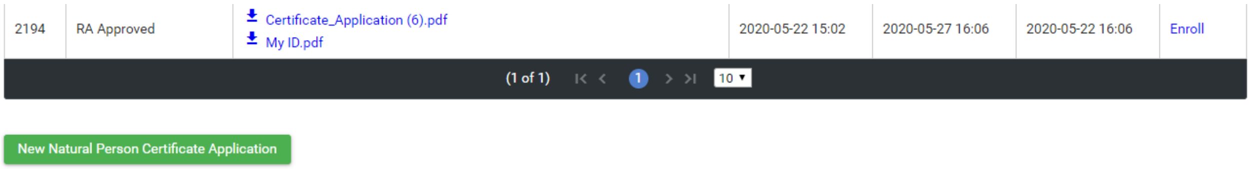
If your application is approved, you will also receive an sms and then you can continue to the next step for issuing and receiving the approved qualified certificate

5. Procedure for the issuance of the Qualified Certificate via Mobile Application

a) For the issuance of the Qualified Certificate visit the below url and choose **“Login”**

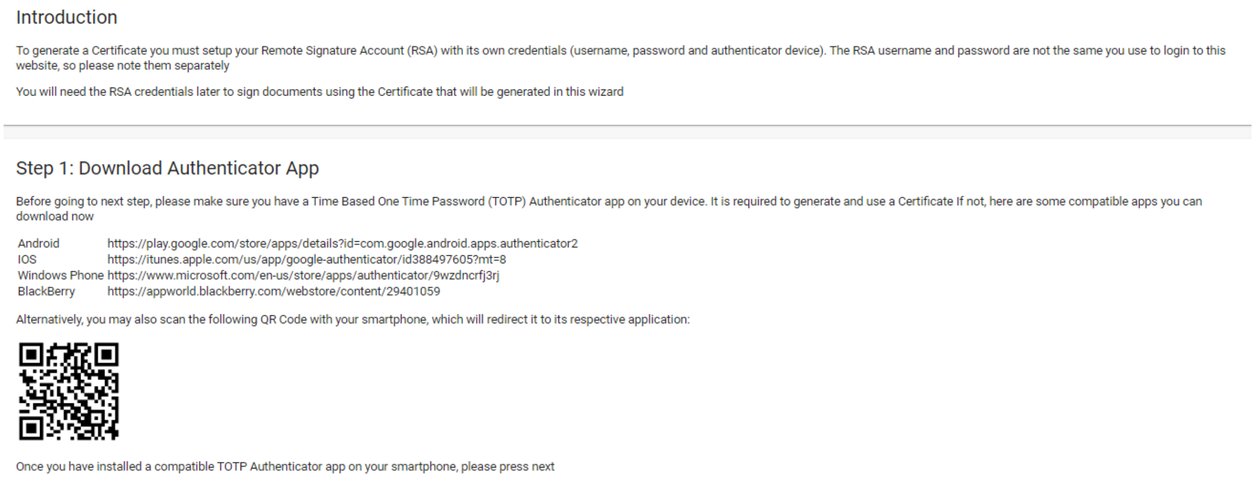
- For real certificates https://aqs-portal.adacom.com
- For test environment https://aqs-portal-test.adacom.com

b) Choose **“My Certificate Applications”**



2194	RA Approved	Certificate_Application (6).pdf My ID.pdf	2020-05-22 15:02	2020-05-27 16:06	2020-05-22 16:06	Enroll

c) In the section on the type of certificate you have applied for, click on "**Enroll**" in the "**Actions**" section.



Introduction

To generate a Certificate you must setup your Remote Signature Account (RSA) with its own credentials (username, password and authenticator device). The RSA username and password are not the same you use to login to this website, so please note them separately

You will need the RSA credentials later to sign documents using the Certificate that will be generated in this wizard

Step 1: Download Authenticator App

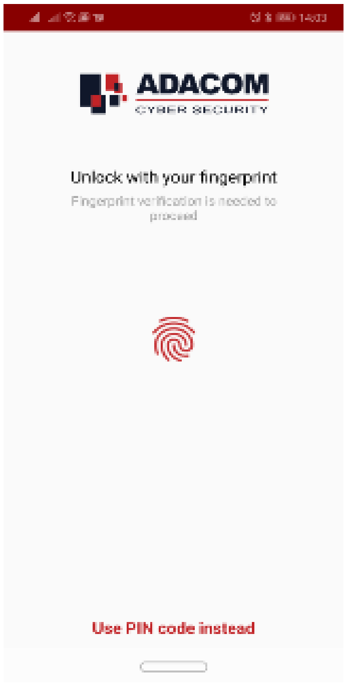
Before going to next step, please make sure you have a Time Based One Time Password (TOTP) Authenticator app on your device. It is required to generate and use a Certificate If not, here are some compatible apps you can download now

Android	https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
IOS	https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8
Windows Phone	https://www.microsoft.com/en-us/store/apps/authenticator/9wzdncrfj3rj
BlackBerry	https://appworld.blackberry.com/webstore/content/29401059

Alternatively, you may also scan the following QR Code with your smartphone, which will redirect it to its respective application:

Once you have installed a compatible TOTP Authenticator app on your smartphone, please press next

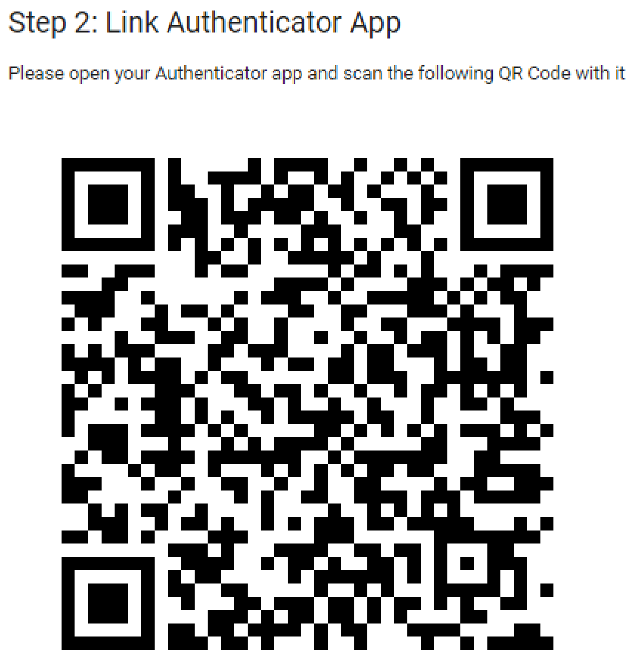
d) **Step 1:** Depending on the type of your device, select the appropriate link and proceed to install the Authenticator App application, as instructed. You can also scan the QR Code with an appropriate application to guide you to the appropriate link



Unlock with your fingerprint

Fingerprint verification is needed to proceed

e) **Step 2**: After you have finished the installation of the application, you will need to scan the unique QR Code using the Authenticator App application

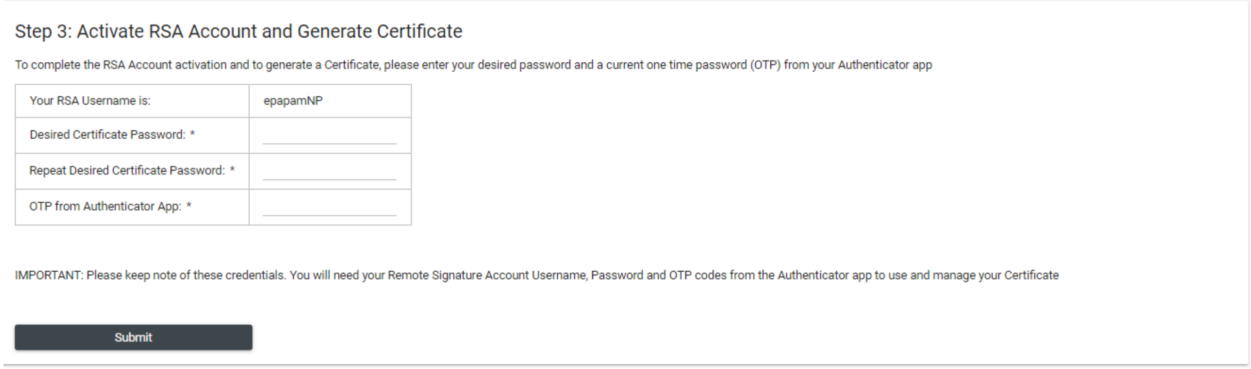


Step 2: Link Authenticator App

Please open your Authenticator app and scan the following QR Code with it

f) **Step 3:** Fill in the form the below:

- **Desired Certificate Password:** Insert a password for your Qualified Certificate
- **Repeat Desired Certificate Password:** Repeat the password for verification
- **OTP from Authenticator App:** Insert the code that you have received via SMS



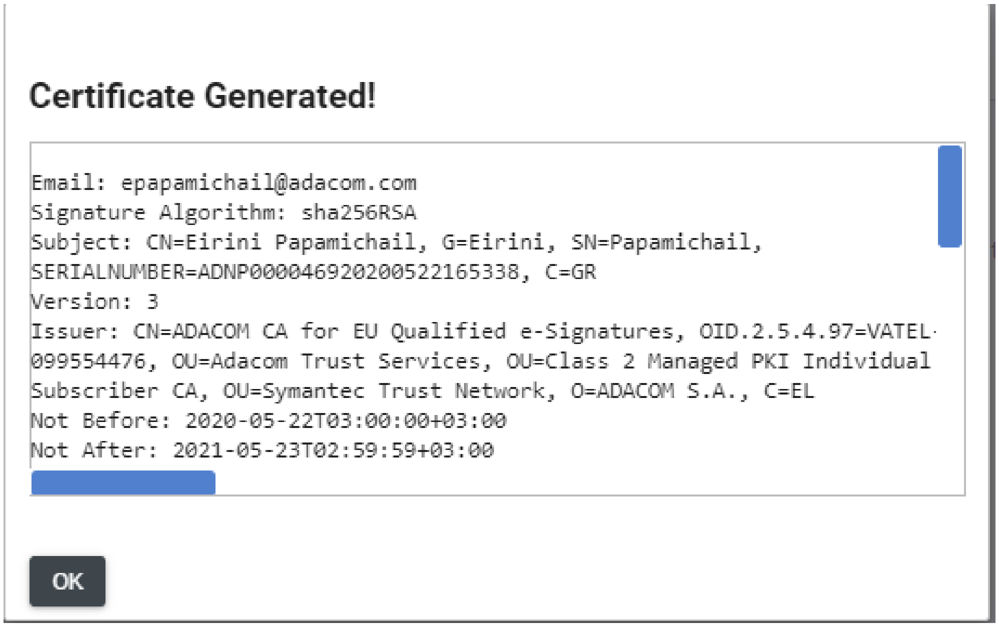
Step 3: Activate RSA Account and Generate Certificate

To complete the RSA Account activation and to generate a Certificate, please enter your desired password and a current one time password (OTP) from your Authenticator app

Your RSA Username is:	epapamNP
Desired Certificate Password: *	
Repeat Desired Certificate Password: *	
OTP from Authenticator App: *	

IMPORTANT: Please keep note of these credentials. You will need your Remote Signature Account Username, Password and OTP codes from the Authenticator app to use and manage your Certificate

<u>Note:</u> The Certificate Password as well as the Remote Signature Application (RSA)- username that has been displayed should be stored securely as it will be necessary for every use of your Digital Signature Certificate



Certificate Generated!

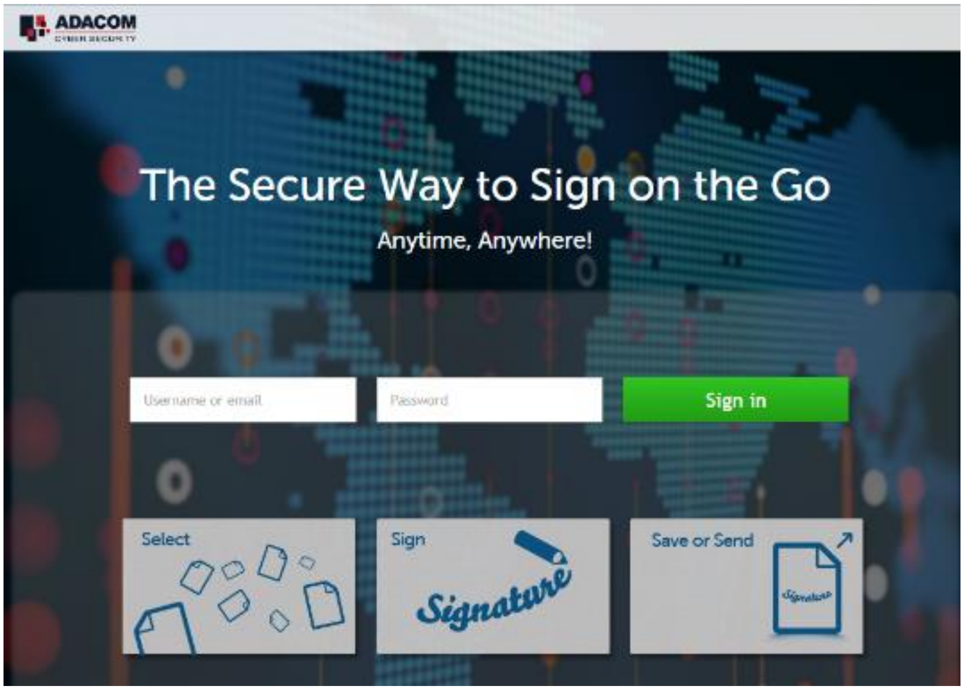
```
Email: epapamichail@adacom.com
Signature Algorithm: sha256RSA
Subject: CN=Eirini Papamichail, G=Eirini, SN=Papamichail,
SERIALNUMBER=ADNP000046920200522165338, C=GR
Version: 3
Issuer: CN=ADACOM CA for EU Qualified e-Signatures, OID.2.5.4.97=VATEL-
099554476, OU=Adacom Trust Services, OU=Class 2 Managed PKI Individual
Subscriber CA, OU=Symantec Trust Network, O=ADACOM S.A., C=EL
Not Before: 2020-05-22T03:00:00+03:00
Not After: 2021-05-23T02:59:59+03:00
```

g) Your qualified certificate has now been generated and is ready for remote use. Click “**OK**” to close the window.

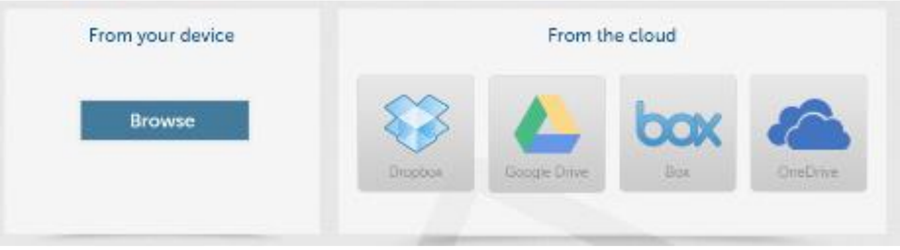
6. Document signing process

a) For the procedure of the remote Qualified Certificate visit the below url and choose **“Login”**

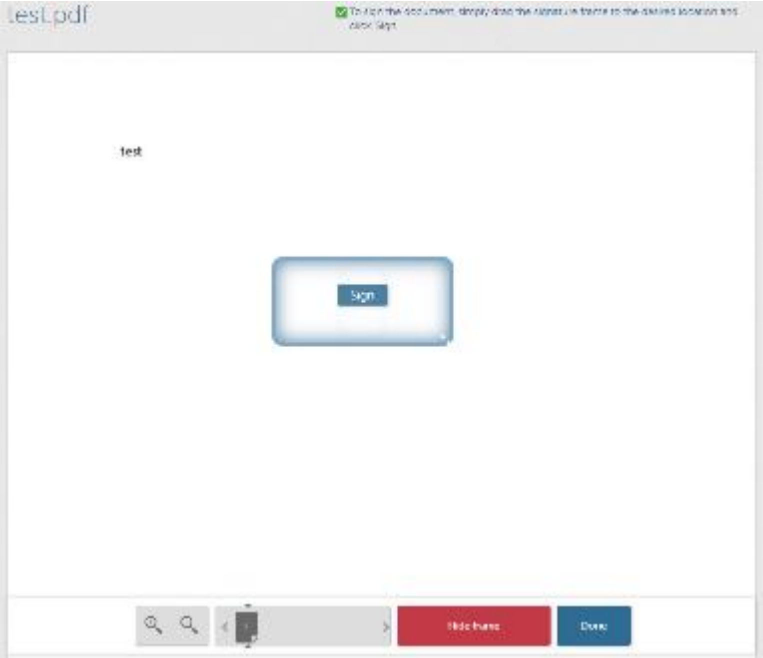
- For real certificates https://aqs-sign.adacom.com
- For test environment https://aqs-sign-test.adacom.com



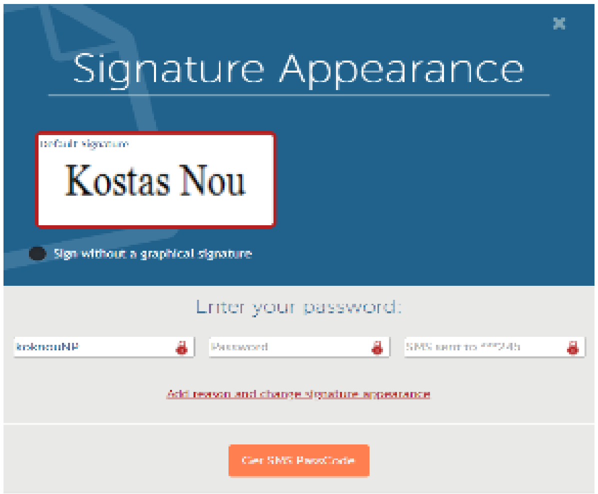
b) Fill in the RSA username displayed and the Certificate Password you chose in the previous chapters, and select **"Sign in"**



c) Using the Browse option, select the pdf file you want to sign. You can select a file locally, or from one of the available cloud services.


To sign the document, simply drag the signature frame to the desired location and click Sign.

d) In the window that appears, specify where you want to place the signature and click on the Sign button.

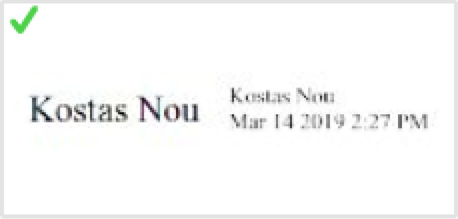


e) You will be prompted to enter the RSA Username, the Certificate password and the 'Extended Password' option where you will insert the OTP password from the mobile application. In case that you have selected the SMS choose “Get SMS Passcode” in order to receive the OTP through SMS.

Note: In case that you have selected the OTP password from the mobile application, please ensure that your mobile device is synchronized to have the network-provided time.

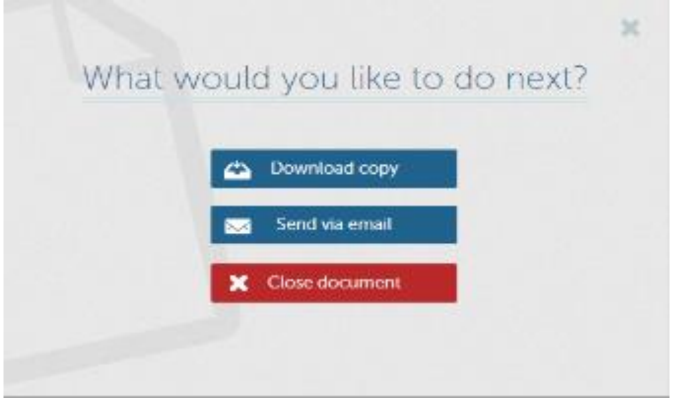
f) Choose **“Apply”**

g) Your signature appears in the document at the point you selected



h) Choose **“Done”** to complete the signing procedure

i) You can choose a copy of the digitally signed document **“Download Copy”**



For more information, please contact with ADACOM support team:
Email: Customer-support@adacom.com
Phone Number: +30 210 9577255