ADACOM

Instructions for the Use of Qualified Certificate for Electronic Signature in a USB token through AQS portal & Video Identification

1. Introduction

This document contains detailed instructions for the registration process on the AQS portal of ADACOM and the process of issuing a qualified certificate for electronic signature of a Natural Person. The validation is carried out first through an automated video call (via dynamic selfie) and in case of six unsuccessful attempts, the user will be referred to a video conference with ADACOM's agent.

You can read detailed instructions about remote identify proofing here.

This solution follows ministerial decision no. 27499/2021.

2. Information about conducting automated video call/video conference with Agent.

Before you start the video process, please:

✓ Make sure you have the required identification documents (ID card or passport) with you. The Greek identity card should contain Greek and Latin characters. If you use a Greek identity card you will have to create a solemn declaration through [gov.gr](gov.gr), detailed information can be found here.

✓ Have an electronic copy of your identification document (identity card or passport). The file should be in photo format (.jpeg, .png, .jpg, .tiff, .bmp).

✓ Check the sound of your computer (microphone, speaker, etc.)

✓ Allow the browser (when you will be asked) to access your microphone and camera.

✓ Make sure that the lighting in your space is sufficient for the needs of the process.

✓ Make sure your network is working properly and your device is connected to the network.

✓ Make sure to close/disable programs on your device that may include sound notifications.

✓ Make sure that nothing will distract you (e.g **no other person appears during the procedure**). You must be alone in the room for the duration of the online video identification.

✓ Estimated completion time: the automated process is about 5 minutes, the video conference with Agent is about 5-15 minutes.

Please note that the success of the automated video call or video conference with Agent may be affected by factors beyond our control, including but not limited to connection or network failure.

2.1 Technical conditions

A prerequisite for the successful completion of the video call is that you meet the minimum technical specifications/requirements described here. Please choose this identity verification method only if you meet the specified requirements otherwise you can choose another identity verification method (for alternative identity verification methods consult the following link).

To conduct the video call:
- ✓ You will need a good internet connection.
- ✓ If you choose to complete the video identification using your computer, we recommend you connect from a private network rather than a corporate network. It is possible that through a corporate network the process may not be completed successfully due to limitations. Otherwise, you can choose to be identified via your mobile phone (see section 5 Mobile identification)
- ✓ Make sure you are disconnected from a VPN, disable any extensions e.g. Ad block.
- ✓ If your network is protected by a firewall, the following IPs and ports should be enabled:

IP Address	Ports	Protocol
54.247.147.109	443, 3478	TCP/UDP
	49152-65535	UDP
54.74.168.39	443, 3478	TCP/UDP
	49152-65535	UDP
108.128.52.90	443, 3478	TCP/UDP
	49152-65535	UDP

A prerequisite for a successful video call is a continuous and high-quality video connection. To achieve this, we recommend that you meet the following criteria:
- ✓ The browser you will use should be Google Chrome (from version v56 and above) or Mozilla Firefox (from version v44 and above) or Edge (from version v80 and above). Microsoft Internet Explorer and Safari on windows are not supported.
- ✓ Desktop cameras often cause problems because their drivers are not adequate and do not have autofocus, i.e they do not focus on the document when it approaches the camera or on the user when he/she tries to validate his/her face.
- ✓ RAM (mobile devices): A memory of 2 GB or more is recommended to ensure that the video process works properly.
- ✓ Internet connection: wired internet connection, minimum bandwidth: 1.5 Mbps or fixed Wi-Fi or 3.5G.s or 4G/5G mobile internet access.
- ✓ Stop programs running in the background (audio and video apps).
- ✓ Allow the program to access your microphone and camcorder.

If during the video call the quality of your connection is not sufficient for the completion of the process, your request will be rejected in order to try again.

3. User registration in the AQS portal

You will need to register on ADACOM AQS portal by following the steps below.

Note: If you already have an account in the AQS portal please follow the instructions in paragraph 4- Login Instructions to your account.
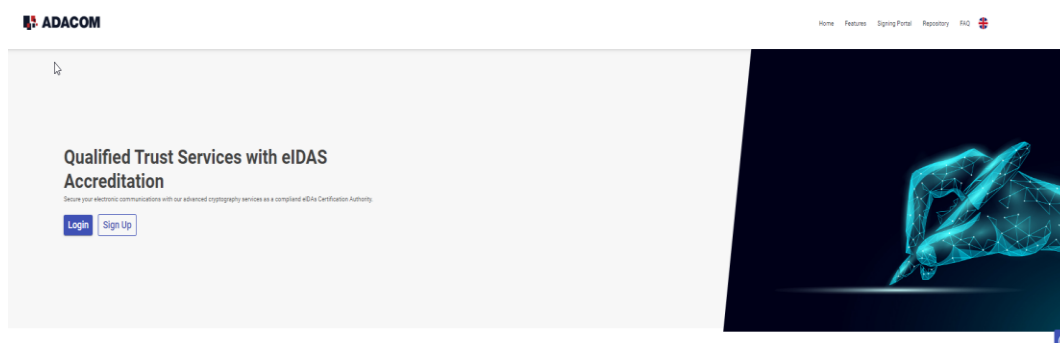
1. Visit the following link and select "Sign Up": ": https://aqs-portal.adacom.com/aqs-portal/landing.xhtml

Figure 1- Adacom's AQS Portal

2. Fill in all the information requested in the Registration Form below and select "**Next.**"

Note: The information you provide must be valid and accurate as it will be used to issue your Qualified Electronic Signature.

Signup Form

Welcome to Aqs portal registration form! Please fill out the following fields to get started.

Email *

Telephone (Mobile) *
Select Country

Telephone (Mobile) *

Username *

Password *

Repeat Password *

Choose a Security Question *

Security Question Answer *

Next →

Figure 2-Registration Form- Account Credentials

3. Complete the creation of your account by filling in the requested information according to the image below and then click **Next**.

Signup Form

Welcome to Aqs portal registration form! Please fill out the following fields to get started.

Name *

Surname *

Name as stated in your Identity or Passport

Surname as stated in your Identity or Passport

Country *
Select Country

ID type *
Select ID type

ID Number *

← Back

Next →

Figure 3-Registration Form- Natural Person Information

4. Scroll down to accept the terms and conditions as well as privacy statement and choose Submit.

documents

Figure 4-Registration Form- Terms and Conditions

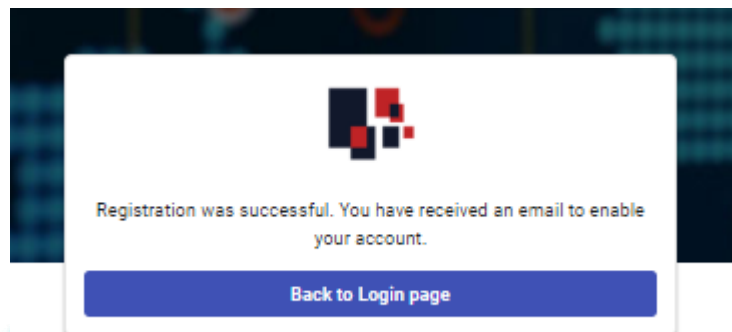5. Your account has been successfully created and you have received an email to activate it.

Image 5-Successful registration

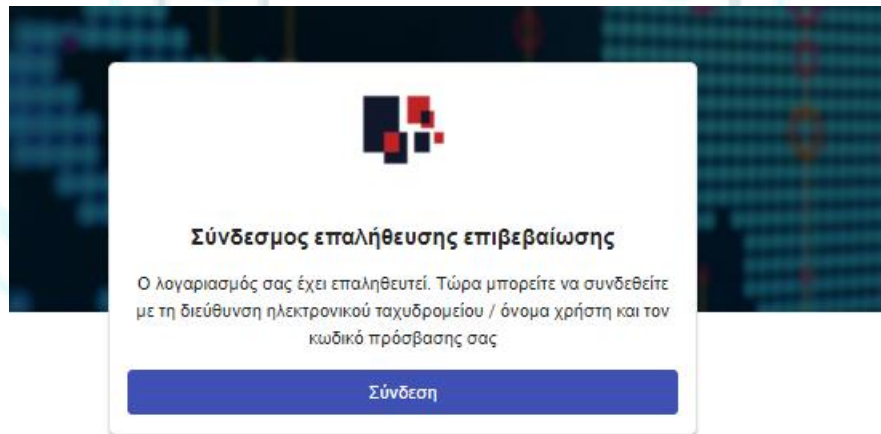6. Once you follow the link in your email, your account will be activated, and you can login.

Figure 6-Account verification

4. Instructions to sign in to your account

1. Visit the following link and select **"Login":** https://aqs-portal.adacom.com/aqs-portal/landing.xhtml enter the **Username or Email** and **Password** you set during your registration in the AQS portal and click **Login**.
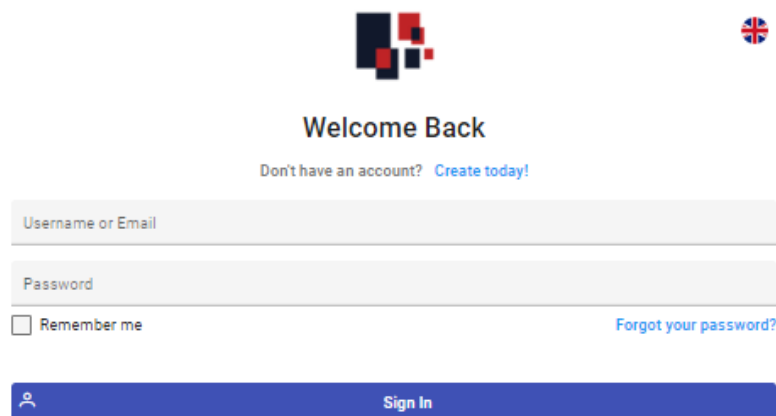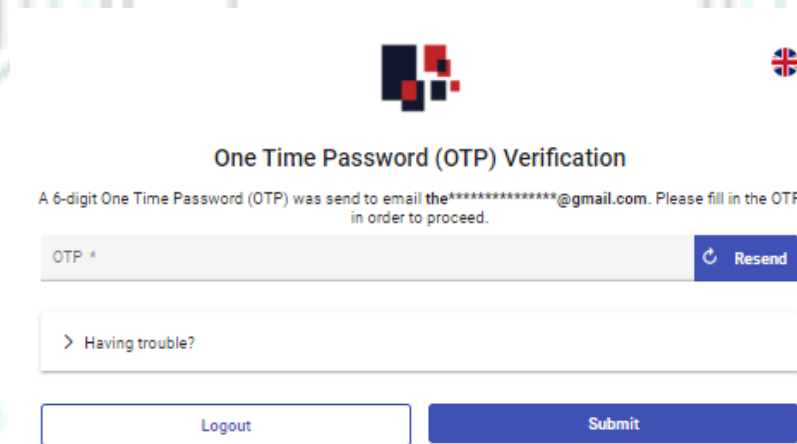
Figure 7-User login

2. An OTP code will be sent to your email, enter it in the relevant field and click **Submit.**

Figure 8 - OTP Verification

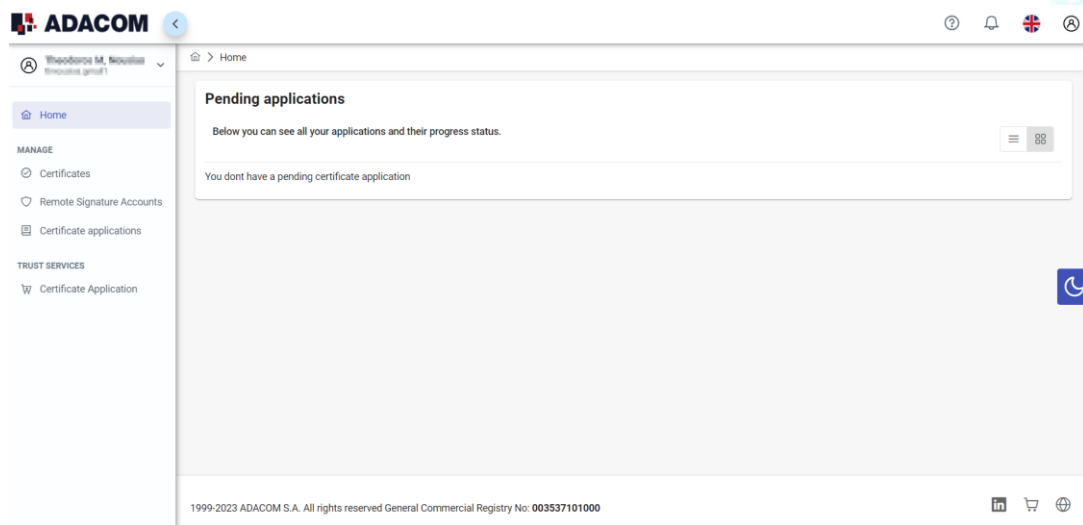3. You have successfully logged into your account. Welcome!

Figure 9- AQS portal Home Page

5. Instructions for submitting your application.

Once you complete your order through the ADACOM e-shop, you will receive in your email the order number as well as the receipt code of your certificate, which you will use in the AQS portal as shown in Figure below.

1. From the left menu you will select the field **Certificate receipt code** and enter the receipt number of your certificate and press **Submit**
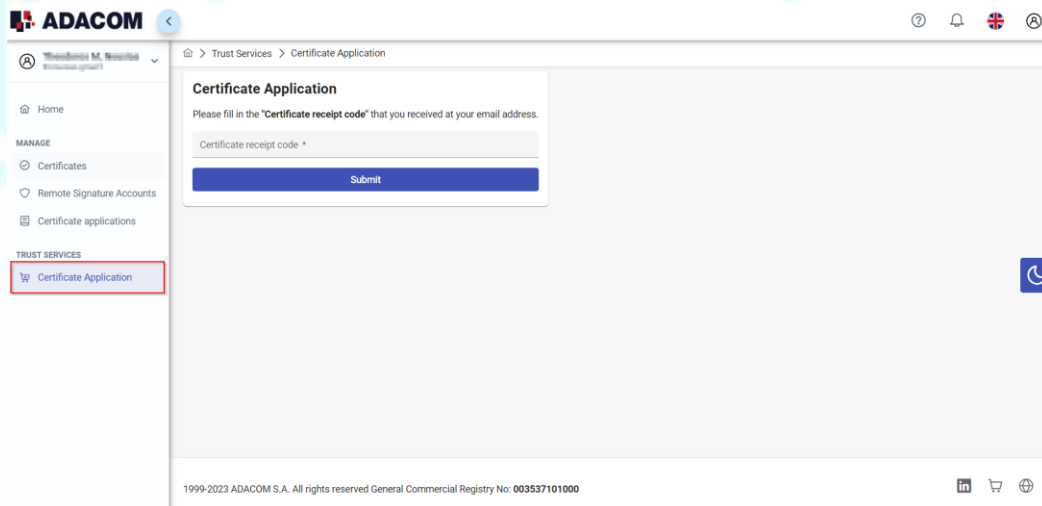
Figure 10 - Electronic Signature Instruction Email

Note for users who want to renew their certificate:

The following action is only performed by users who already have an active qualified certificate for electronic signature that is expires soon.

To renew your certificate, you must select from the left menu: My certificates and then the Renewal Certificate button as shown below:

When you click on Renew you will see the field to enter the certificate receipt code you received via email.
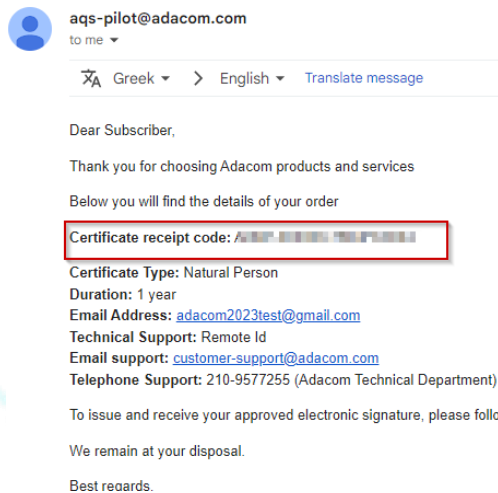
The email you receive is like the following:

Figure 11-Certificate Receipt Number

2. You will then see the information about your order details and you can select the "**Next**" button to continue.
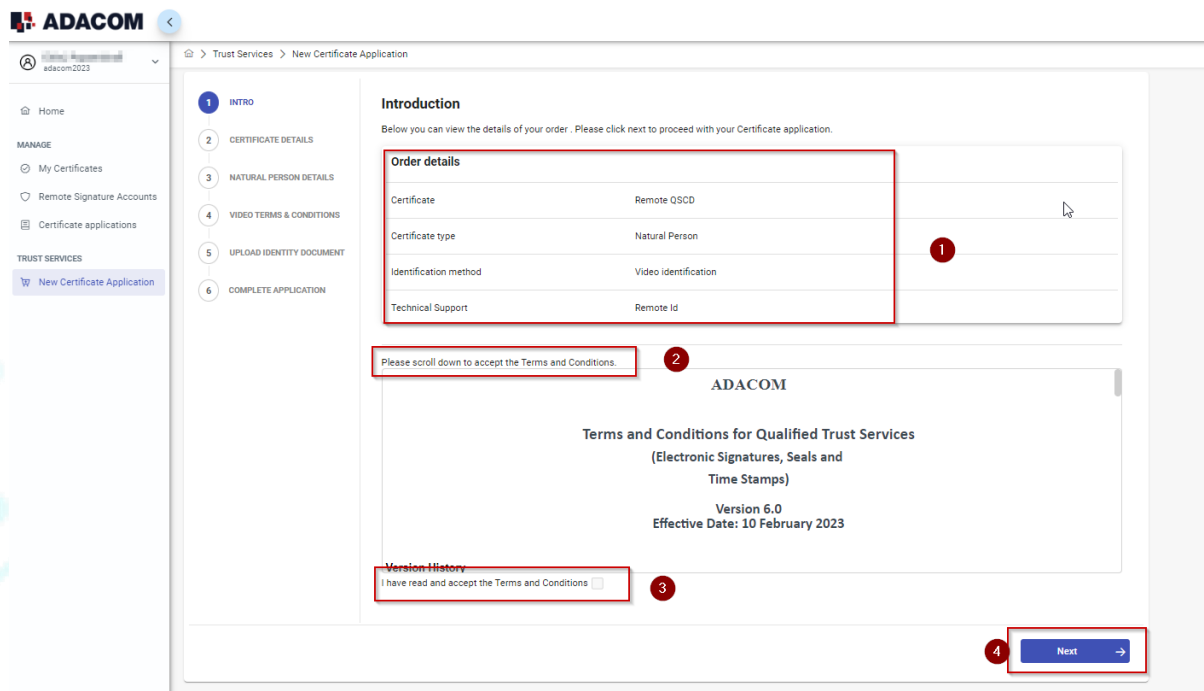

Figure 12-Order Details

3. In the certificate information you will need to select one of the following options for the Serial number of the certificate and click **Next**:
   o Default (recommended)
     If you choose the default, the serial number of your certificate will be a random code.
   o Id or passport

If you select ID card, the serial number of your certificate will be your ID or passport number. (in case your ID card contains Greek characters that do not correspond to the Latin characters e.g. Ψ, Θ, Σ, Λ, Φ etc., select the default).
- o **VAT number (Tax information)**
If you choose a VAT number, the serial number of your certificate will be your VAT number.

Figure 13- Certificate Information

4. In the Natural Person's Information, you will see your details filled in (they have been filled in automatically during your registration).
You will need to confirm that your personal data is correct, and in case you find an error in any of the fields, you can correct them from here.
For example, your full name should appear in the same way as it appears on your passport or ID card, otherwise your application will be rejected.

Figure 14- Form for filling in data

5. You should then read and accept the Terms and Conditions related to remote identification and select **"Next"**.
   Note:
   In case you have chosen Greek Identity Card as your identification document:
   Visit the following link
   https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/psephiaka-eggrapha-gov-gr/ekdose-upeuthunes-deloses to create and save locally on your computer a solemn declaration certifying your identity, then select the "Upload File" field to upload this document to the platform.

Text of Solemn Declaration
The text you should enter in the Solemn Declaration to ADACOM is:
I declare that the above information is true and accurate and I want to issue a qualified certificate of electronic signature.

Figure 15- Remote Identification Terms & Conditions

The list of acceptable ID document is also available here (pages 8-10).

6. The system will then ask you to upload your copy of your ID or passport in image format. You will have to press "**Select front image**", **"Select back image"** and once uploaded select "**Next**".

   Note: You can't upload a .pdf file in this field

You can upload your identification image in png, jpeg, jpg, tiff, gif or bmp format.
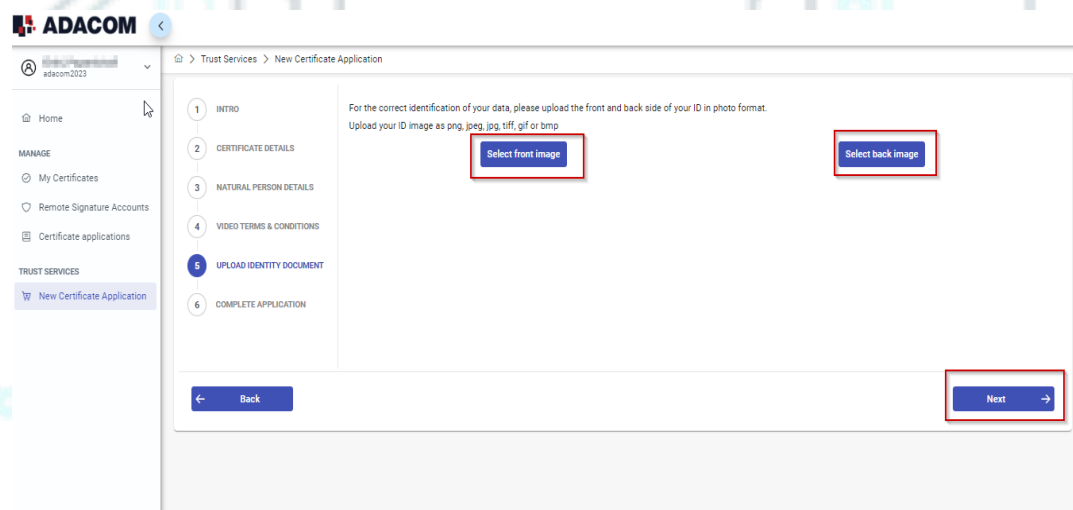

Figure 16-Submission of an identification document

7. At this stage your application is completed. At the same time, you can proceed with your video identification by selecting "**Start video identification**" or if you want you can complete it in a second time.
    If you choose at this stage to complete video identification, please follow the instructions below in Start Video Identification.
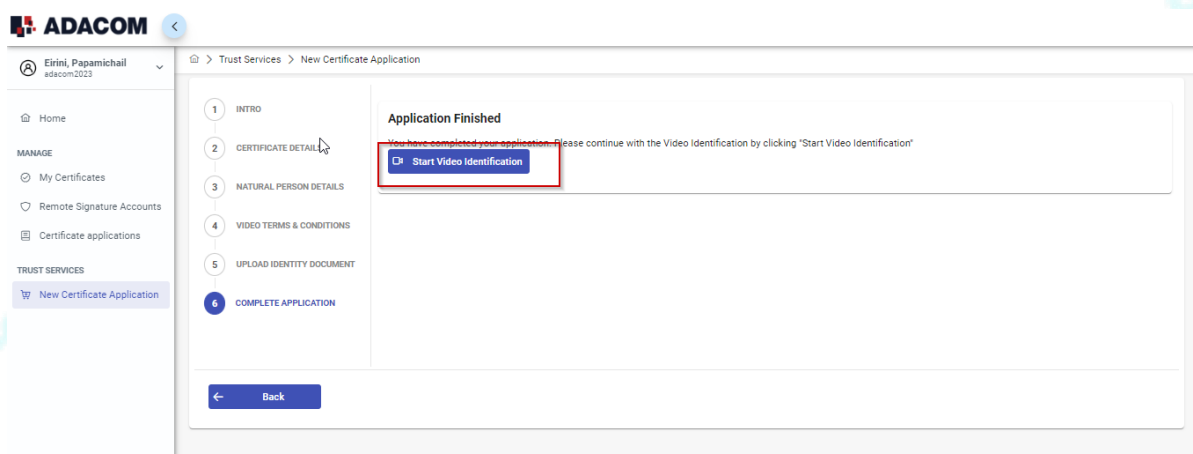

Figure 17-Application completion

8. In case you complete your video identification <u>later</u>, you can select "**Home**" from the left menu and then the green button **"Start identification with Video**"
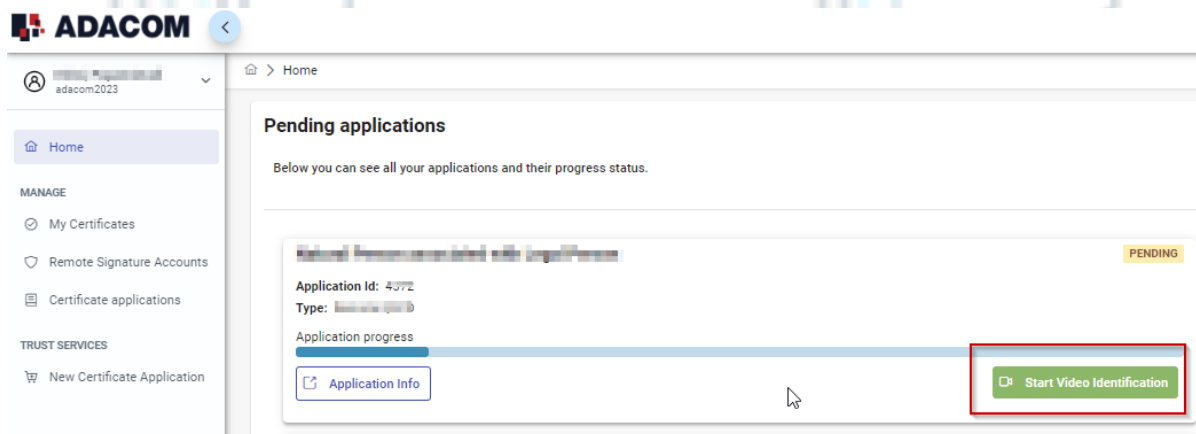
Figure 18-Start video identification

In addition, at any time you wish you can view the details of your application from the option "**Application Information**" (without being able to edit them). Also, by choosing the button "Download your application" you can download your application form and by choosing the button "Upload file" you can upload files related to your application.
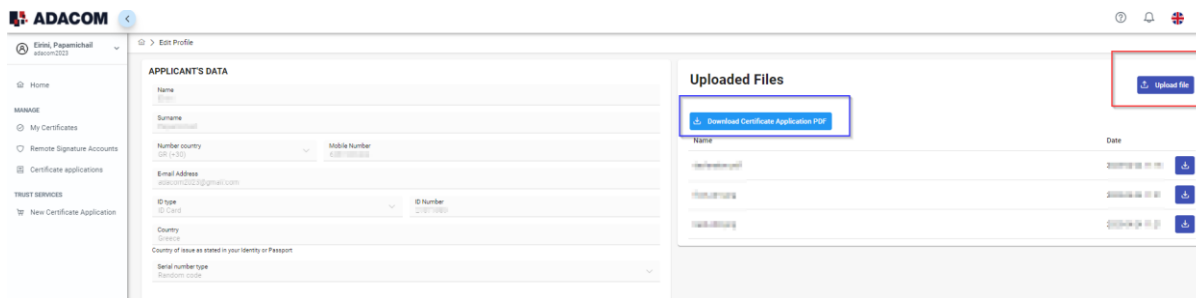

Figure 19-Application Information

6. Start video identification.

1. In the option below if you select " **Use your mobile phone"** to conduct the video identification using your mobile device.

   Otherwise, you can continue to the device you are already connected and select **"Use this device"** then click **"Next".**
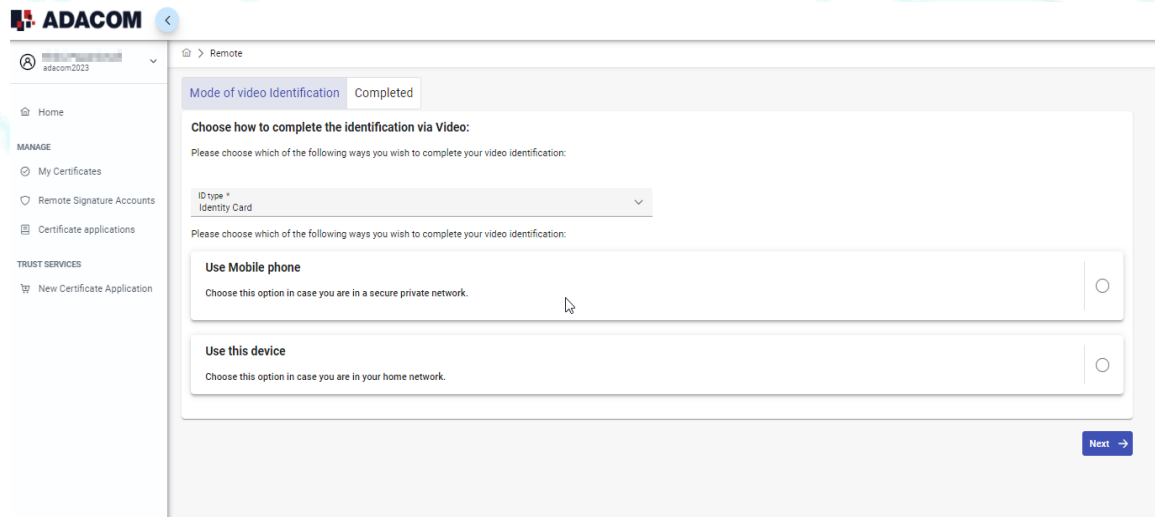

Figure 20-Select video conferencing mode.

2. The system will ask you to present your ID to the camera. You'll need to follow the instructions you read to your screen and place your ID card in the suggested aera. Once your ID has been successfully identified, you will be asked to get close to the camera. At this stage you will need to move your hand in front of your face and smile.
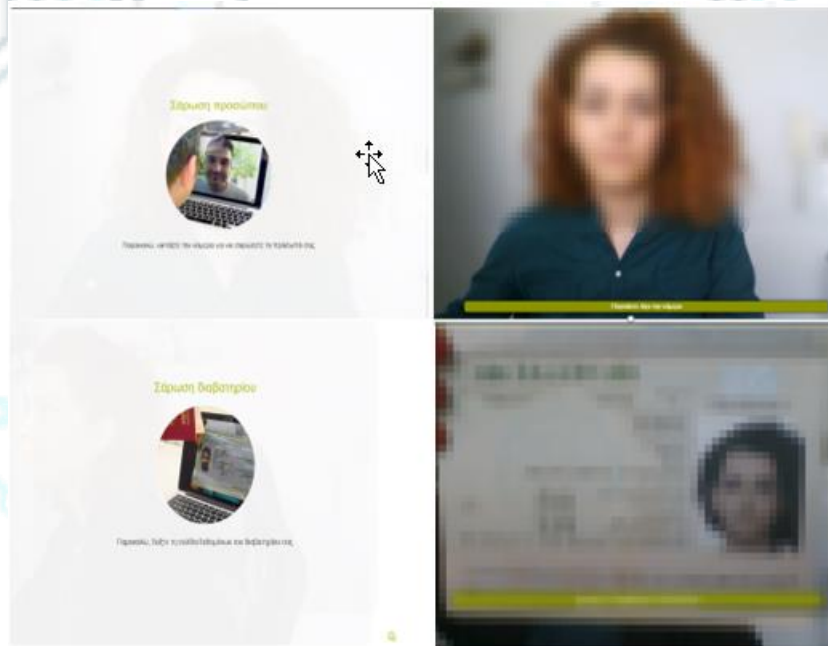
Figure 21-Identification document & face recognition

Identification via mobile device

3. If you choose to conduct the video identification through your mobile phone, you can either scan with your mobile the QR code that will appear on your screen or select **"Send SMS"** in order to receive via sms the link of the portal.
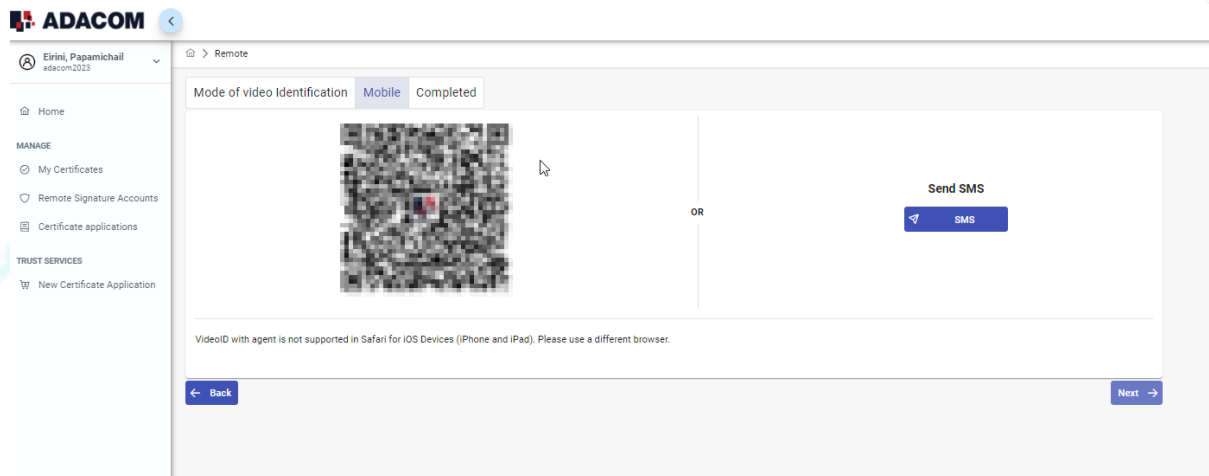

Figure 22-Video identification via mobile device

4. The system will ask you to present your ID to the camera. You'll need to follow the instructions you read to your screen and place your ID card in the suggested aera. Once your ID has been successfully identified, you will be asked to get close to the camera. At this stage you will need to move your hand in front of your face and smile.

Figure 23-Identification document & face recognition via mobile

5. At a random point during identification, you will see a random captcha code which you will must fill in the relevant field to continue.
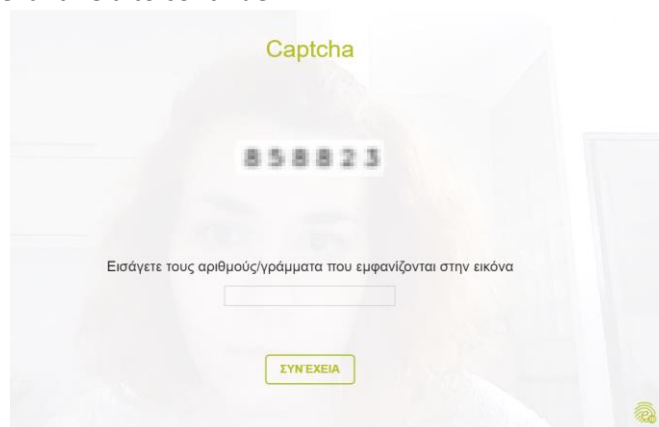

Figure 24-Captcha import

6. Once the identification of your ID and your face is successfully completed, the system will ask you to verify your mobile phone number. Once you receive the OTP on your mobile phone, you can fill it and choose "**Next**".
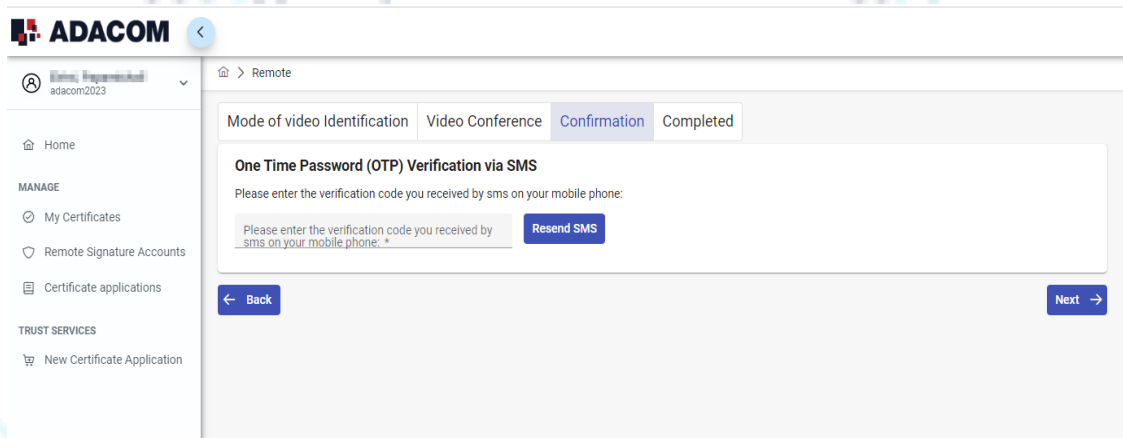
Figure 25- Verification via OTP

7. Finally, you select the "**Complete**" button.

Process of your Application.

Your application is being processed and will be reviewed by ADACOM's LRA/RA department:

➢ If your identification is successful, LRA/RA will approve your request and you will receive an email and sms notification to your mobile phone in order to proceed with the steps described in paragraph 7.

➢ If your verification is not successful, the LRA/RA department will reject your request and you will have to repeat the process following the steps from the beginning of section 4 (Start Video Identification).

➢ If you make multiple failed automated video call attempts, then the system will show you the option to make an appointment for Video Conferencing with an employee. See the instructions in (Video conferencing with employee).

Video conferencing with an employee

8. The Subscriber has the option of teleconferencing with an ADACOM employee, where communication takes place in real time "face to face".
In this case, an appointment with an ADACOM employee is required at a predetermined available date and time, which is arranged through your AQS portal account.
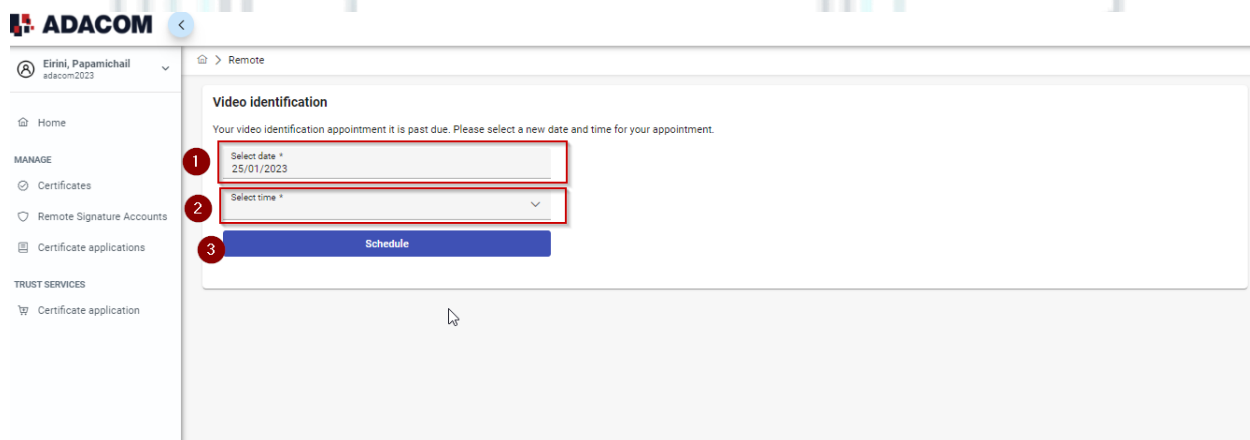
Figure 26- Appointment with agent

- The video conference's duration is about 5 to 15 minutes.
- Available video conference hours are daily from 09:00 am to 16:45 pm (GR time), excluding holidays.

If your verification is not successful, LRA/RA will inform you of the reason for the rejection as well as with the alternative identification methods which can be viewed here.

7. Instructions to activate your electronic signature.

To issue and activate your qualified electronic signature login to your portal account, and follow the steps below:

1. From the left menu select **Home** and then click button [Enroll] on your RA approved application**.**
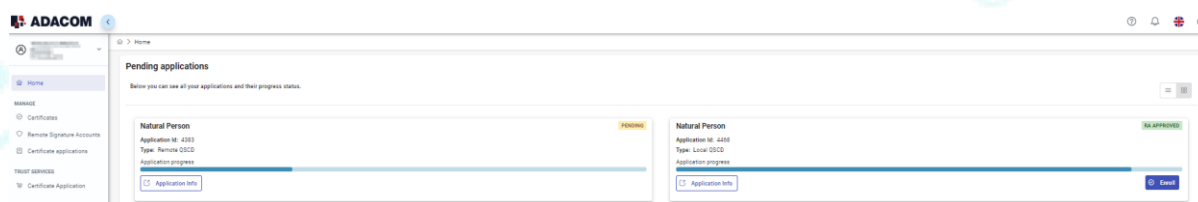

Figure 27 - List of submitted applications.

Step 1. Follow the link to download the SafeNet Authentication Client (SAC). Then install the program leaving the Default options active.
Step 2. Insert the USB token to the port of your computer.
Step 3. Follow the link to download the Adacom USB Client and install the program.

2. After completing the steps above, return to the portal and select next.
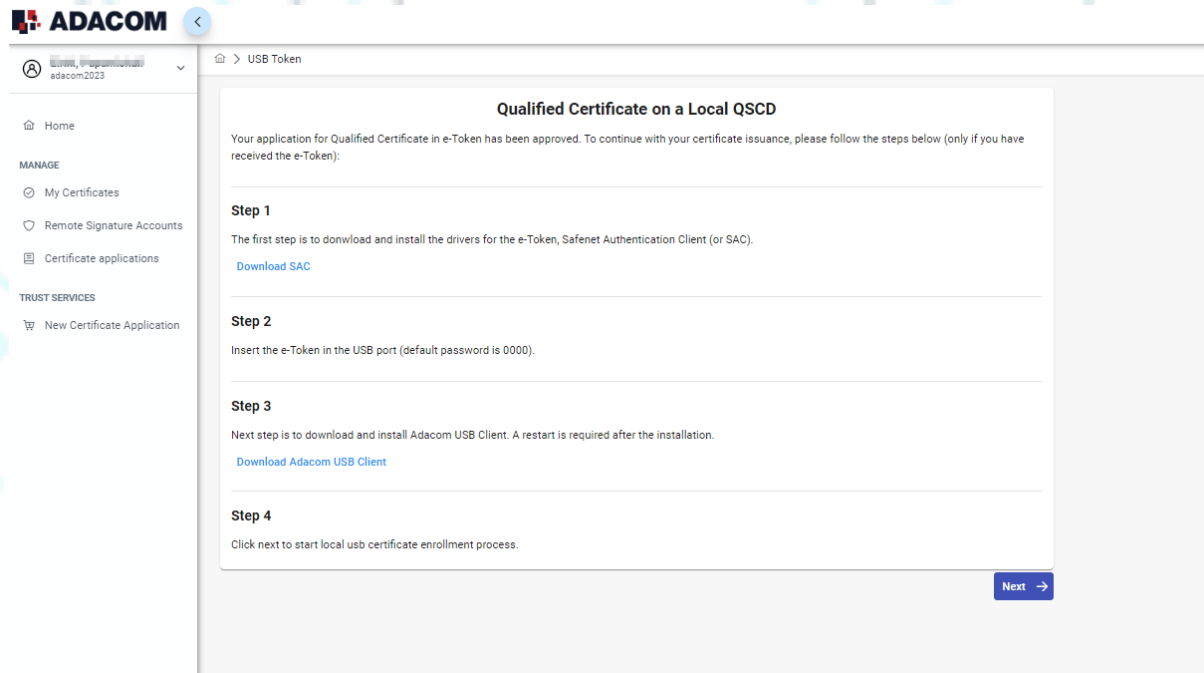

Figure 28 - Certificate Activation Part 1

3. In the next screen, click "**Launch Client**" and select "Open" in the window that will appear at the top of the page. After the Program Status changes to "Connected" you can proceed with "**Find e-Token**". Once that connects as well, select "Next" to proceed.
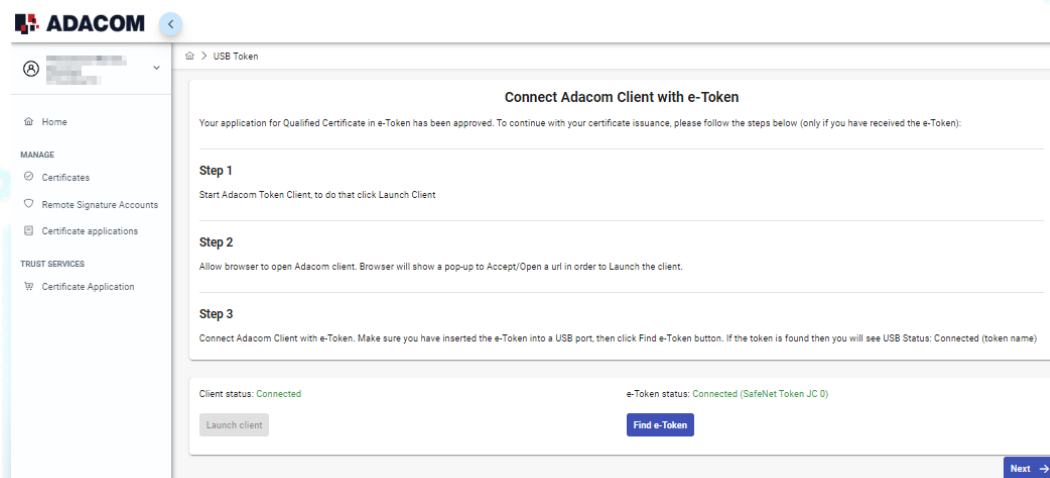

Figure 29 - Launch Client & Find E-Token

Kreontos 25, GR 10442 Athens

http: www.adacom.com

email: customer-support@adacom.com

20 | Page.

4. In the final stage of the enrollment process, you will need to do a final check of your details, and make sure everything is correct. (If you notice any errors, please notify customer-support@adacom.com before continuing further). Next, you will be prompted to fill in the Token password which is set by default as: **e-Token Pin: 0000**. Submit it and click **Import Certificate.**

    ❖ **In case of renewal, please insert your personal token password.**

Figure 30 - Import Certificate

5. After that you will be prompted to fill in your digital signature pin, which is set by default as: **Digital Signature Pin: 000000**, two consecutive times. Submit it both times and click Ok.

    ❖ **In case of renewal, please insert your personal signature pin.**

Figure 31 - Digital Signature Pin

6. Your Certificate has been issued and imported successfully. Click the following link for instructions about how to sign a document on Acrobat reader and how to use timestamp.
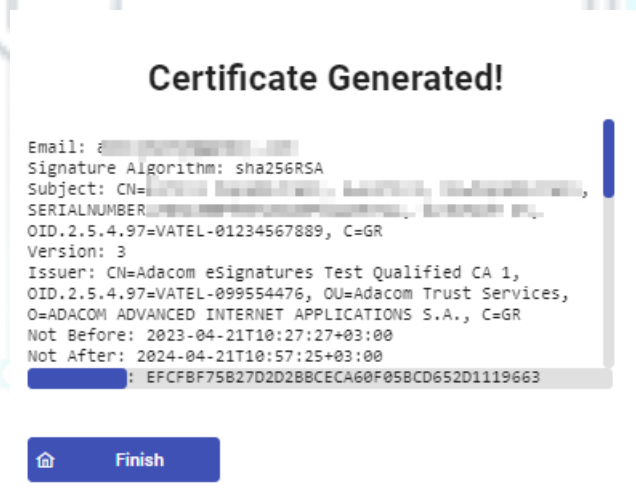
Figure 32-Certificate Generated

7. From the option "My certificates" that you will find on the left menu, you can see the information of each certificate (its details, expiration date, validity etc.) Through this option you can also manage your certificate by downloading the certificate or revoke it if it is necessary.
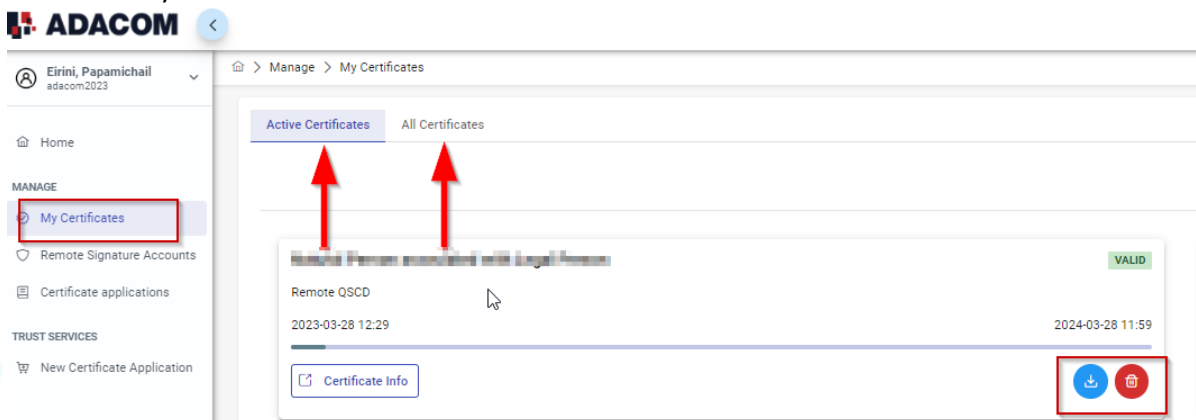

Figure 33-My Certificates

8. Instructions to change usb token password and digital signature pin.

Once you have successfully received your certificate, you will need to change the usb token passwords from its default ones to set the codes that only you will know.

Caution:

➢ **you should not change the default administrator password and default signature puk**.

➢ In case of changing them, you should know the codes you have set.

➢ If you lock your usb token and do not remember the administrator password and puk you will not be able to use your usb token or your signature.

➢ In this case your Usb token should be replaced with a new one.

Steps to change token password.

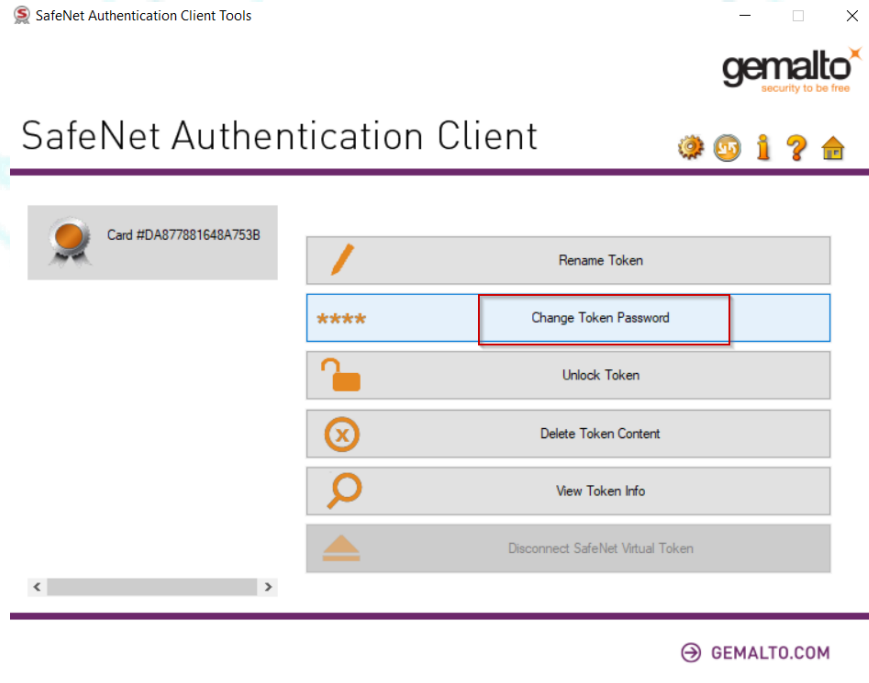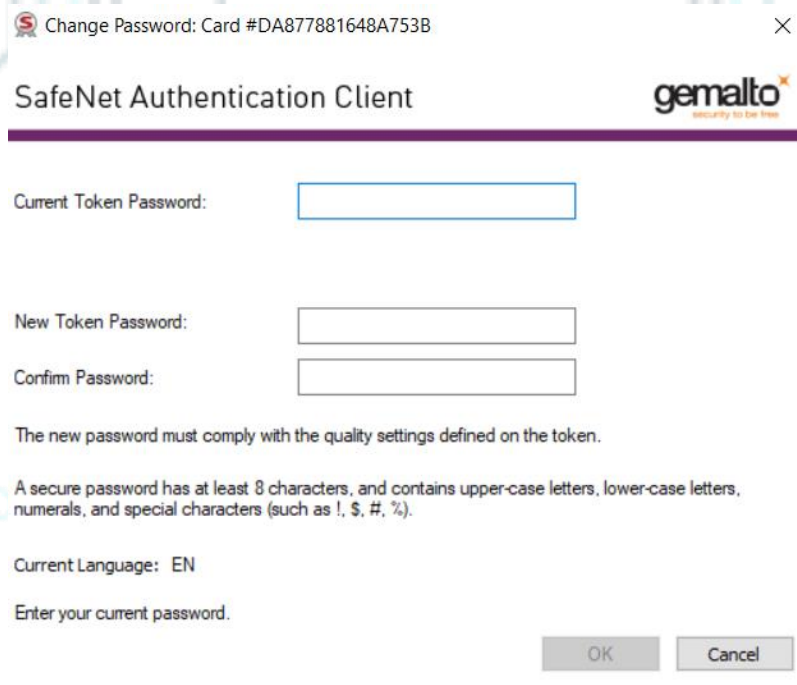➢ Open the SafeNet Authentication Client Tools and choose Change token Password.

Figure 34-Change token password

➢ At the current token password put: **0000 (4 zeros) and then set the new token password.**

Figure 35-Change token password

Figure 36-Change token password

Steps to change digital signature pin.

➢ Open SafeNet Authentication Client Tools 🔵 and choose Advanced View ⚙, Set digital
signature pin ✳, fill in the default digital signature PUK: **000000**, and click ок. Finally, set
your personal pin (Note: At this point, you can set the same password as the token
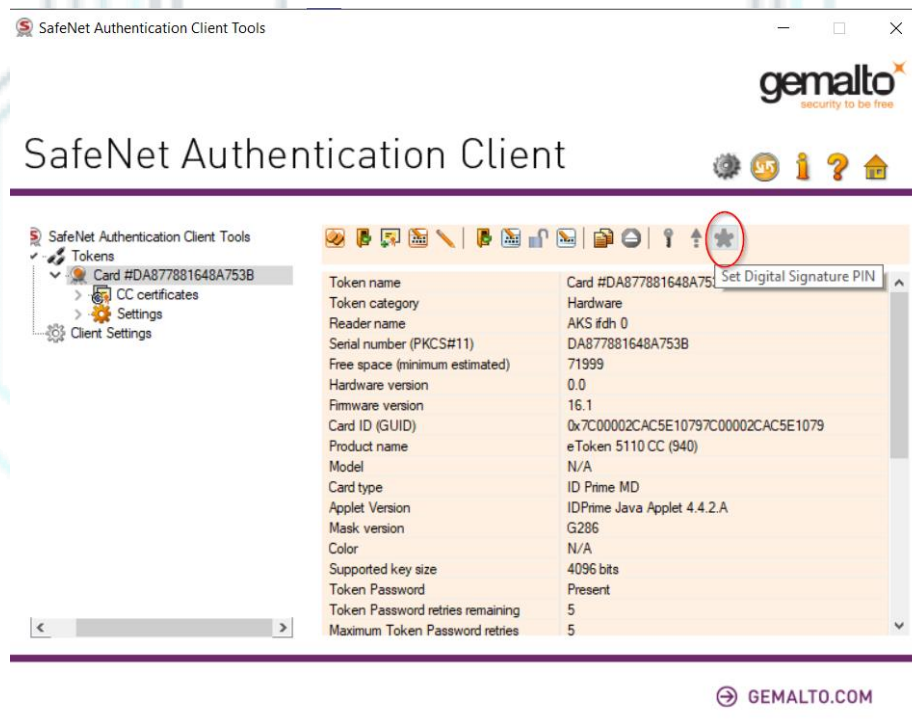password for your convenience).
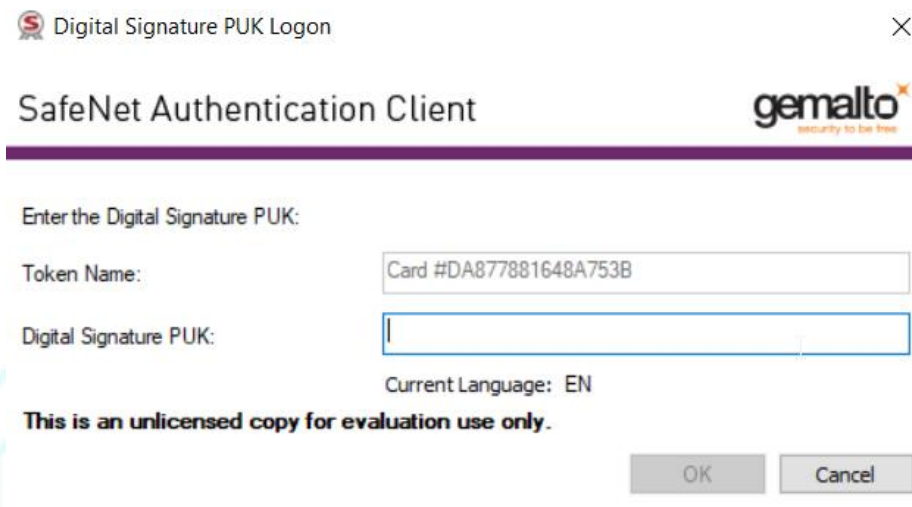
Figure 37-Change digital signature pin

Figure 38-Change digital signature pin

➢ **For your convenience, we recommend you to set the same password with this one you have set in your token password.**

Set PIN: Card #DA877881648A753B ✕

SafeNet Authentication Client

gemalto
security to be free

New Digital Signature PIN: [   ]

Confirm PIN: [   ]

☐ Token PIN must be changed on first logon

The new PIN must comply with the quality settings defined on the token.
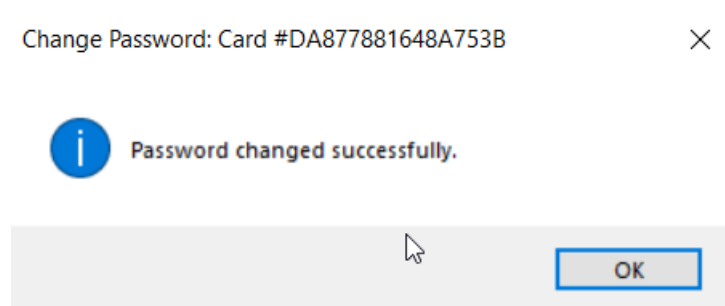
A secure PIN has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

Current Language: EN

Enter a new PIN.

[OK] [Cancel]

Figure 39-Change digital signature pin