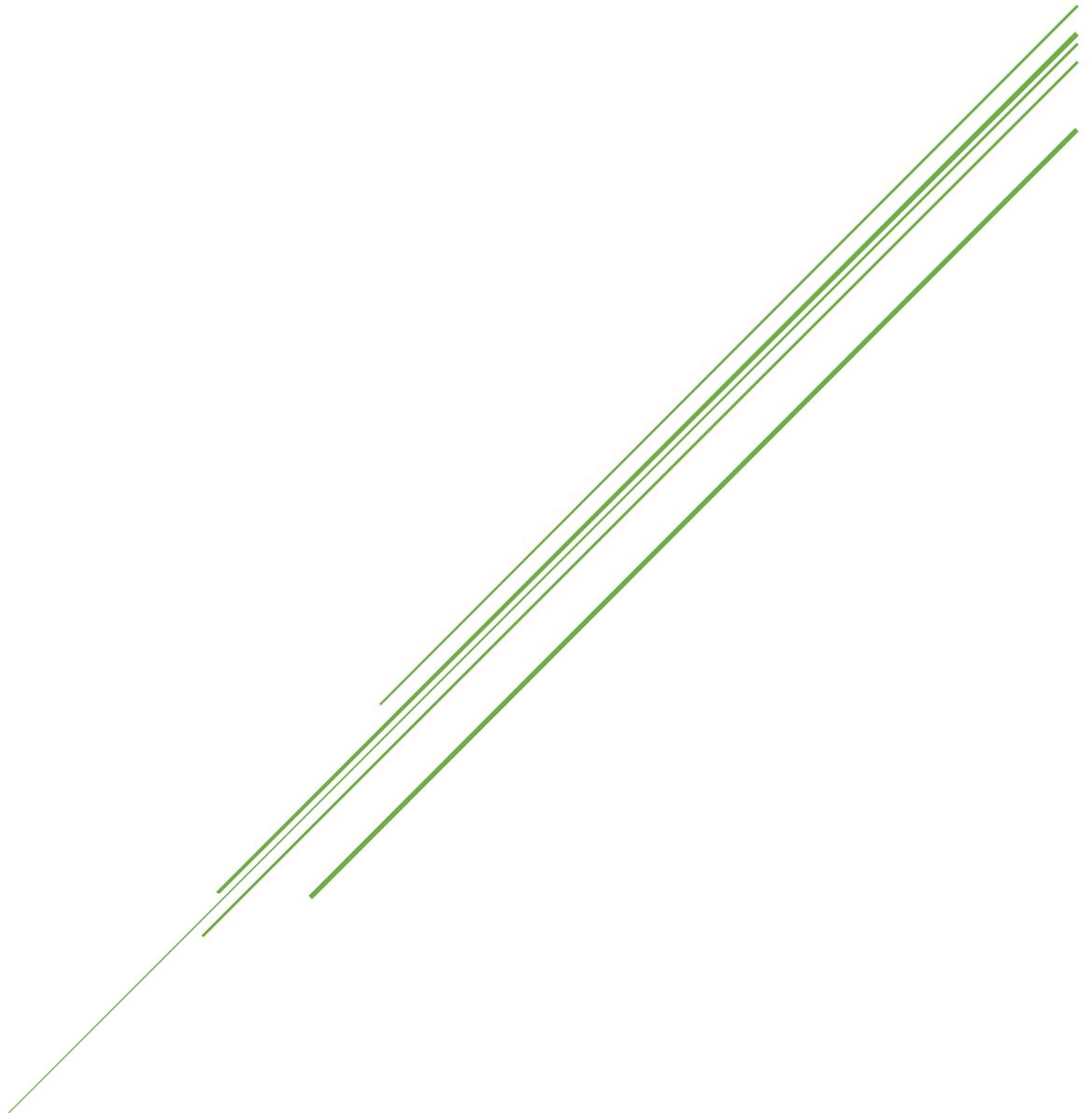


# QUALIFIED ELECTRONIC SIGNATURES

**Request & issue your Qualified Electronic Signature**



## Contents

1. Introduction .....	2
2. User Portal Registration & Log-in.....	2
2.1. Registration Procedure .....	2
2.2. Login Procedure .....	4
3. Certificate Application Procedure.....	6
4. Approval of the issuance of the Qualified Certificate.....	9
5. Procedure for the issuance of the Qualified Certificate .....	10
6. Download JCC Authenticator .....	12

# 1. Introduction

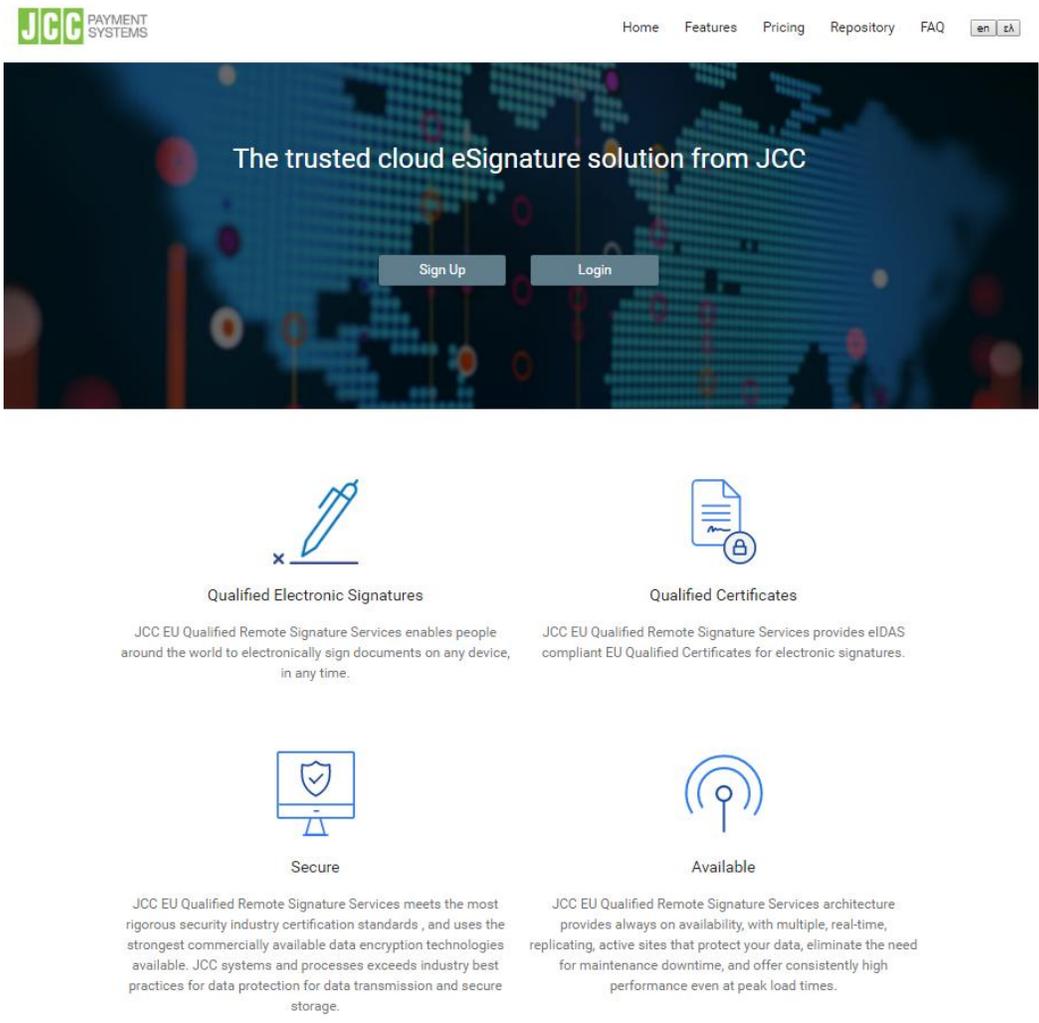
This document is a digital certificate enrolment guide. You may find the information required, as well as a step-by-step guide for obtaining an EU Qualified Certificate remote signature.

## 2. User Portal Registration & Log-in

The first step is to create an account to the JCC Trust Services Portal.

### 2.1. Registration Procedure

- a) To register, using any browser **visit** <https://trust.jcc.com.cy> and choose **“Sign Up”**



b) Fill in the following fields

Note: Use Latin characters only. The information should be valid, as this data will be used for your certificate application

Sign-up Field	Values
Username	Username must be at least 5 characters long (20 max) and may only contain letters, numbers and periods
Email	Enter your email address. An account confirmation email will be sent to this email address
Title	Choose from the list
First Name	Must be exactly as stated in your ID/ Passport
Last Name	Must be exactly as stated in your ID/ Passport
Country	Must be exactly as stated in your ID/ Passport
Address	Enter your mail address
Postal Code	Enter the postal code of the address above
Telephone (Fixed Line)	Optional
Telephone (Mobile)	Select Country and enter your mobile phone number
ID type	Choose from the list
National ID or Passport Number	Must be exactly as stated in your ID/ Passport
Password	Password must be at least 8 characters long and must contain characters from three of the following four categories: <ol style="list-style-type: none"> <li>1. Uppercase Latin alphabet characters (A-Z)</li> <li>2. Lowercase Latin alphabet characters (a-z)</li> <li>3. Arabic numerals (0-9)</li> <li>4. Nonalphanumeric characters (for example, !\$,%)</li> </ol>
Security Question	Choose from the list and answer a security question. This question can be used for your identity verification through phone.
Terms and Conditions	Scroll down and check the box to agree with JCC's Terms & Conditions
Privacy Statement	Scroll down and check the box to agree with JCC's Privacy Statement
reCaptcha	Check the box "I'm not a robot"

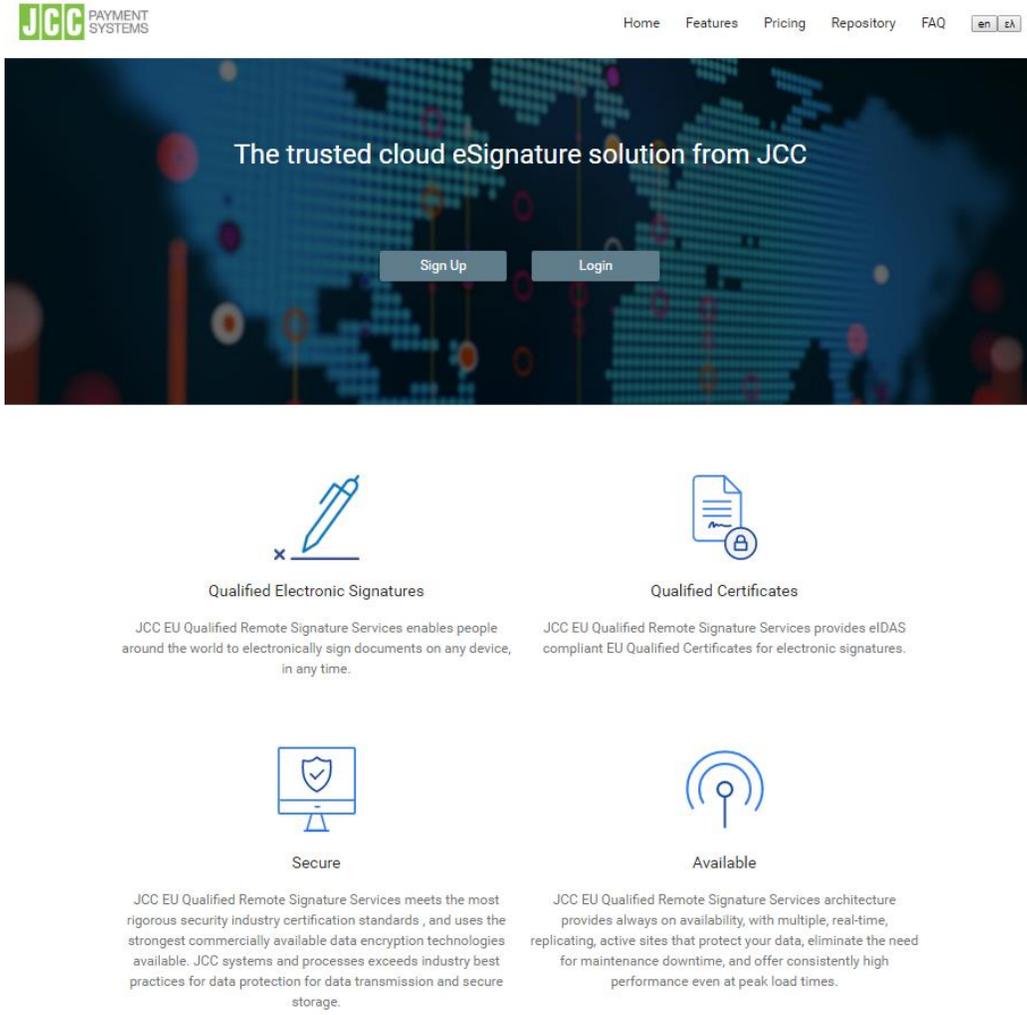
c) Click on "**Submit**". A confirmation email will be sent to the provided email address.

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

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

## 2.2. Login Procedure

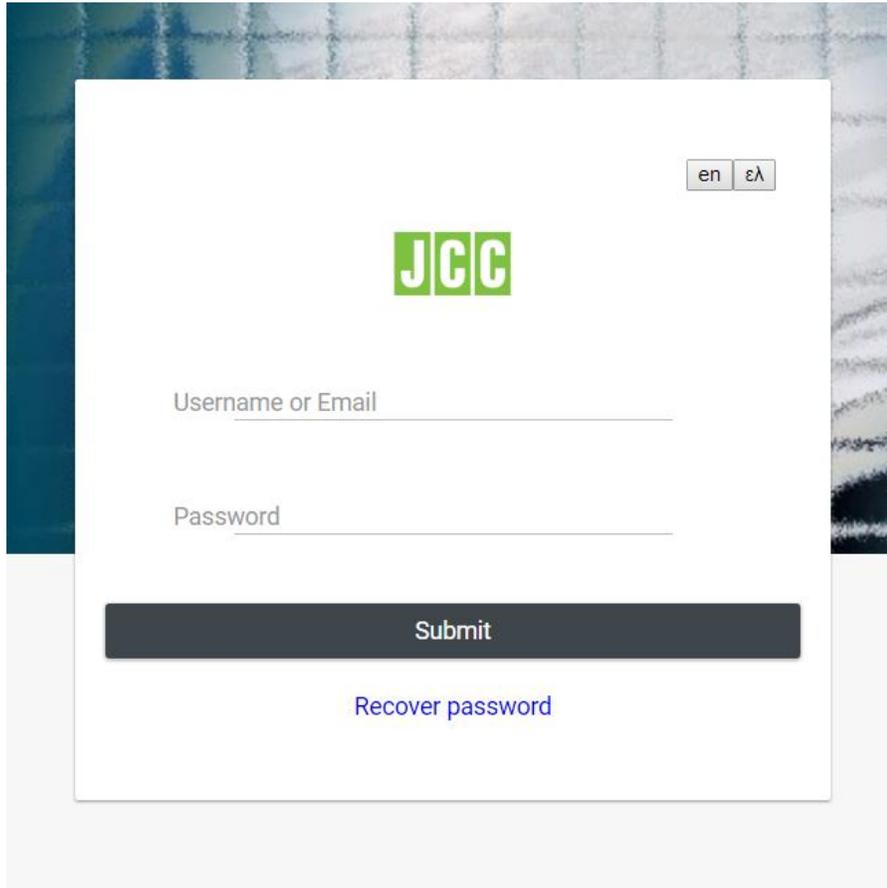
- a) Using any browser **visit** the JCC Trust Services Portal at <https://trust.jcc.com.cy>
- b) Choose **“Login”**



The screenshot displays the JCC Payment Systems website. At the top left is the JCC logo with 'PAYMENT SYSTEMS' underneath. To the right are navigation links: Home, Features, Pricing, Repository, FAQ, and language options 'en' and 'za'. The main banner features a world map background with the text 'The trusted cloud eSignature solution from JCC' and two buttons: 'Sign Up' and 'Login'. Below the banner are four service highlights, each with an icon, a title, and a description:

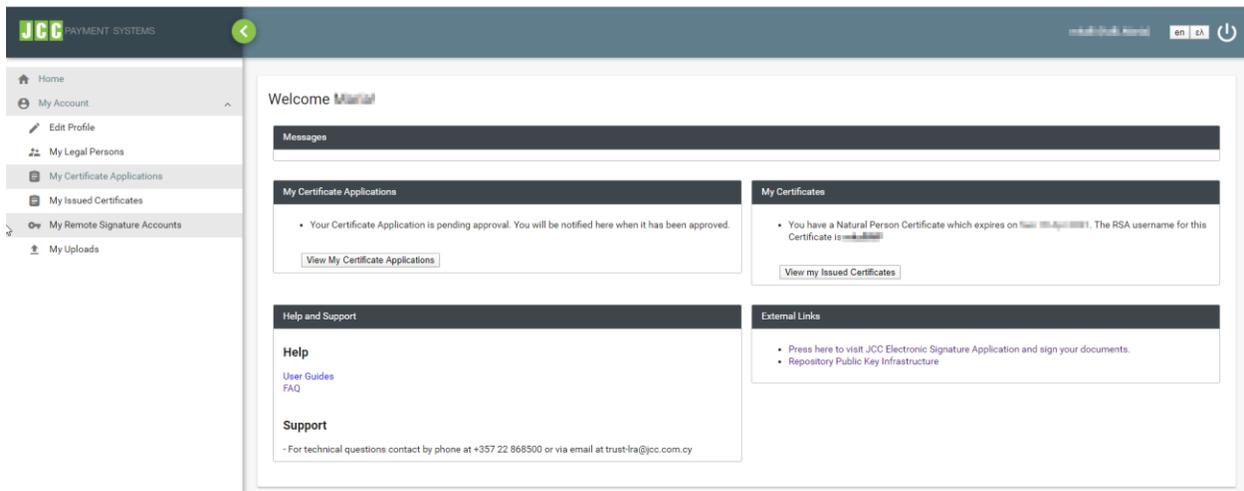
- Qualified Electronic Signatures**: JCC EU Qualified Remote Signature Services enables people around the world to electronically sign documents on any device, in any time.
- Qualified Certificates**: JCC EU Qualified Remote Signature Services provides eIDAS compliant EU Qualified Certificates for electronic signatures.
- Secure**: JCC EU Qualified Remote Signature Services meets the most rigorous security industry certification standards, and uses the strongest commercially available data encryption technologies available. JCC systems and processes exceeds industry best practices for data protection for data transmission and secure storage.
- Available**: JCC 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.

c) Provide your **username** and **password** and click on “**Sign In**”



The image shows a login form for JCC. At the top right, there are language selection buttons for 'en' and 'ελ'. In the center is the JCC logo, which consists of the letters 'JCC' in white on a green square background. Below the logo are two input fields: 'Username or Email' and 'Password'. A dark grey 'Submit' button is positioned below the password field. At the bottom of the form, there is a blue link that says 'Recover password'.

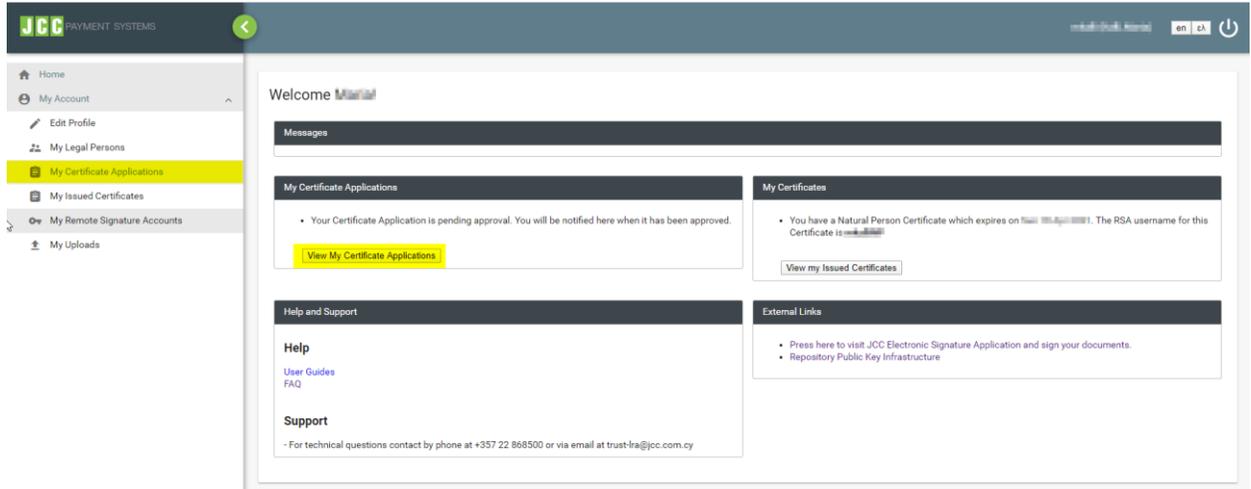
Now you have entered to your portal account and you should be looking at the following screen.



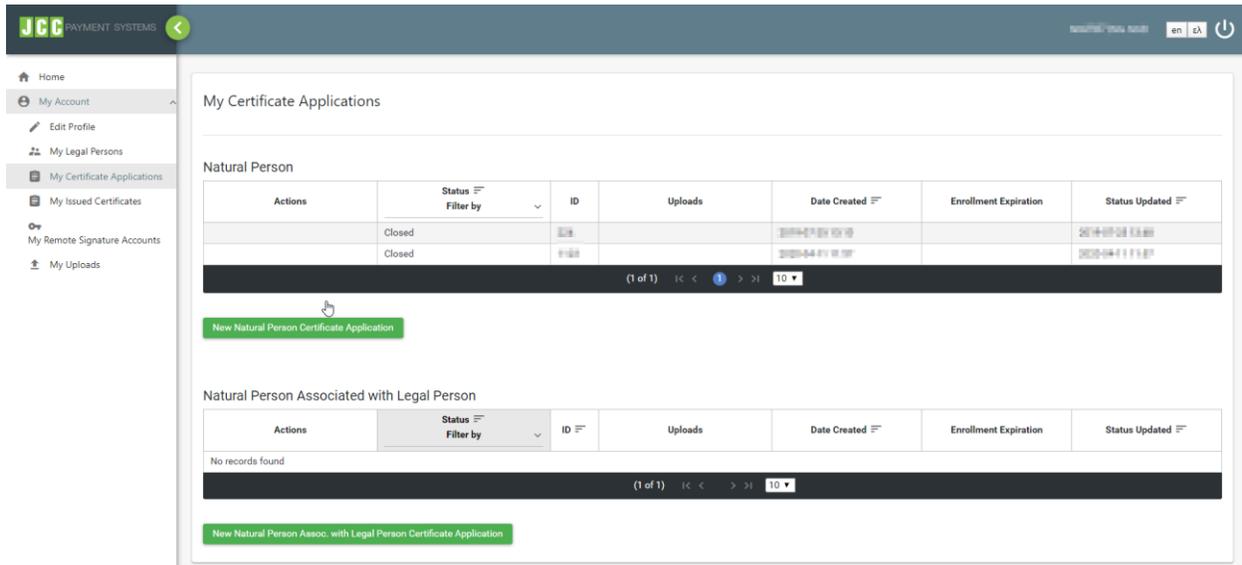
The image displays the JCC portal dashboard. The top header includes the JCC logo and 'PAYMENT SYSTEMS' on the left, and navigation icons and language buttons on the right. A left sidebar menu contains links for Home, My Account, Edit Profile, My Legal Persons, My Certificate Applications, My Issued Certificates, My Remote Signature Accounts, and My Uploads. The main content area is titled 'Welcome' and features several sections: 'Messages', 'My Certificate Applications' (with a pending application notification and a 'View My Certificate Applications' button), 'My Certificates' (with a certificate expiration notice and a 'View my Issued Certificates' button), 'Help and Support' (with links for User Guides and FAQ), and 'External Links' (with links to JCC Electronic Signature Application and Repository Public Key Infrastructure). A support contact number and email are provided at the bottom of the Help and Support section.

### 3. Certificate Application Procedure

- a) To create a Certificate Application, **select** “My Certificate Applications” on the left panel or “View My Certificate Applications” on the main screen.



- b) Select the type of certificate you want to request:
- New Natural Person Certificate Application
  - New Natural Person Associated with Legal Person Certificate Application



- c) Check the validity of your information. You may edit any data necessary. Your First, Last Name and Country must match your ID or Passport.

**APPLICANT'S DATA**

Position: Mr

First Name: John

Last Name: Doe

Country: Cyprus

Address: [Empty]

Post Code: [Empty]

Telephone Number (Fixed Line): [Empty]

Telephone Number (Mobile): [Empty]

Email Address: [Empty]

ID Type: ID Card

ID Number: [Empty]

Please scroll down to accept the Terms and Conditions.

I have read and accept the Terms and Conditions \*10

- d) Scroll down to read the JCC’s Terms & Conditions and check the box to confirm that you agree.
- e) Click **“Next”**
- f) Click **“Certificate Application PDF Download”** to download the certificate application you created in pdf format.

**1. Select OTP Authentication Method 2. Application Form 3. Download and Sign PDF**

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

**Certificate Application PDF Download**

and visit JCC Payment System Local Registration Authority:

JCC LRA  
Stadiou 1, 2571 Nisou  
Nicosia, Cyprus  
Tel: (+357) 22 868 500  
Email: trust-lra@jcc.com.cy

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

**+ Choose File(s)** **Upload file** **Cancel**

**Finish**

g) Open the PDF file and:

- In case you do not have a valid EU Qualified Certificate for electronic signatures you will have to

i. print the document and visit:

JCC LRA  
Stadiou 1, 2571 Nisou  
Nicosia, Cyprus  
Tel:(+357) 22 868 500  
Email: trust-lra@jcc.com.cy

ii. or send by courier service or post office to JCC LRA the following documents:

- a copy of the ID or passport certified by Citizens' Service Centers or District Administration and
- the signed application form certified by a Certifying Officer, Citizens' Service Centers or District Administration.

In case the Subscriber resides in any country other than Cyprus and Greece, the documents must be validated through the Apostille procedure.

- In case you do have a valid EU 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**”

h) Click “**Finish**”

As soon as your Certificate Application and Proof of Identity documents have been reviewed successfully by the JCC Local Registration Authority (LRA) and JCC Registration Authority (RA), you will be notified via email and you will be able to continue to acquire your digital signature (4).

## 4. Approval of the issuance of the Qualified Certificate

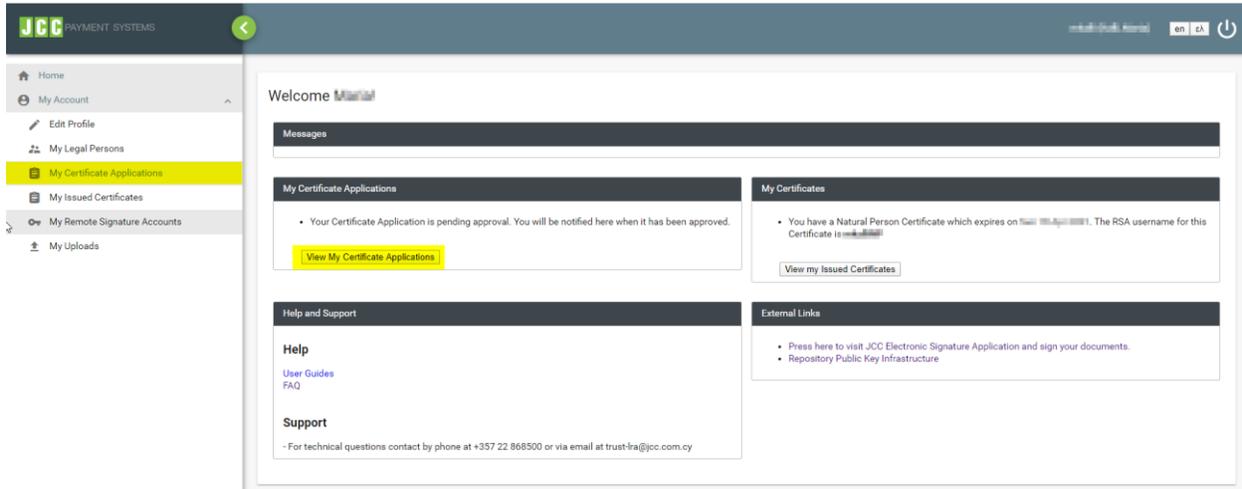
There will be a process of confirming the details of the application and identifying the user data from JCC, and then you will receive an email update on whether your application was approved or rejected.

This process might take up to **3 business days.**

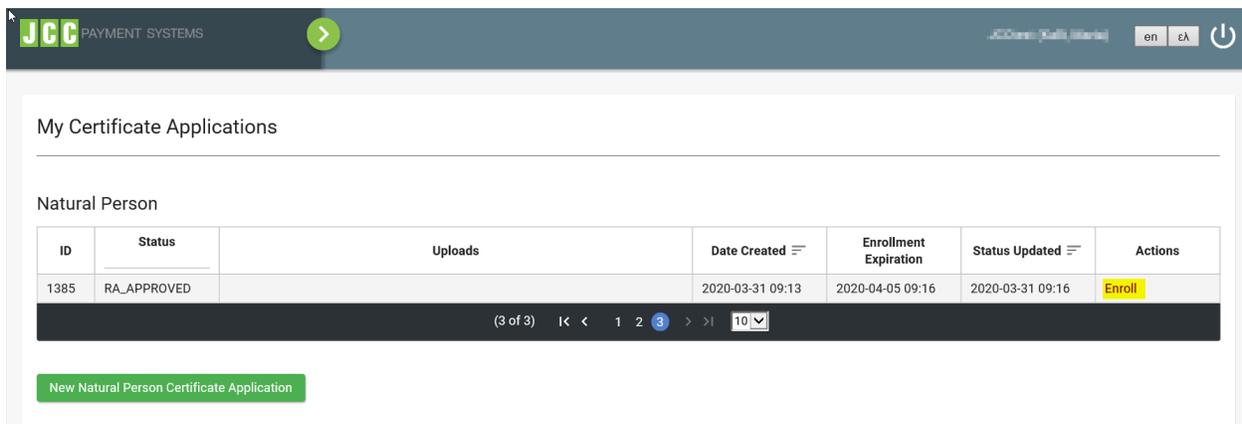
If your application is approved, continue to the next step for issuing and receiving the approved digital certificate.

## 5. Procedure for the issuance of the Qualified Certificate

- a) To receive the Certificate, select **“My Certificate Applications”** in the main screen or **“View My Certificate Application”** the left panel.



- b) Find the certificate and click on **“Enroll”** in the **“Actions”** section



- c) Fill in the form the below:
- **Password:** Insert a password for your Qualified Certificate.
  - **Repeat Password:** Repeat the password for verification

## Introduction

To generate a certificate, you must setup your Remote Signature Account (RSA) with its own credentials (User ID and Password). 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 with your certificates.

## Step 1. Activate the RSA account and Generate Certificate

To complete the RSA account activation and to generate a Certificate, please enter your desired username and password.

User ID	JCCtest
Password *	<input type="password"/>
Repeat Password *	<input type="password"/>

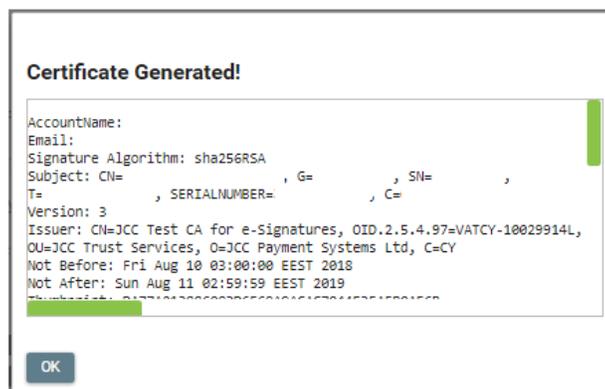
Note:

-Please keep note of these credentials for future use.

Submit

**Note:** The Certificate Password as well as the User ID that has been displayed should be stored securely as it will be necessary for the usage of your Digital Signature Certificate.

- d) Your certificate has now been generated and is ready for remote use.



## 6. Download JCC Authenticator

In order to be able to use the issued certificate from previous step for document signing, you have to download and register the JCC Authenticator application to your mobile device.

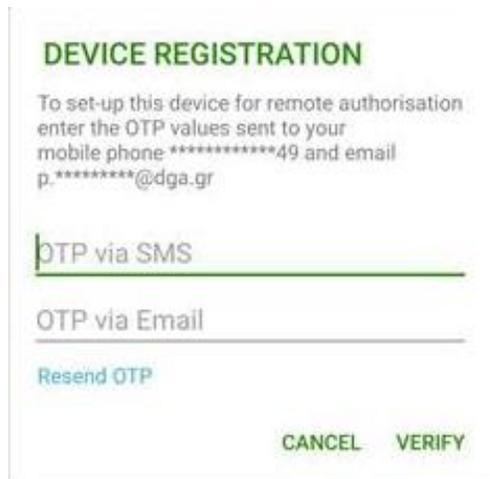
- a) Download the Mobile RAS App using your mobile phone device



- b) Open the Mobile RAS App and enter your User ID you used on Step 1 and click "NEXT" to login



- c) Enter the two OTPs that you will receive through email and SMS to the corresponding fields and click "VERIFY"

A screenshot of a "DEVICE REGISTRATION" screen. The title "DEVICE REGISTRATION" is in green. Below it, text reads: "To set-up this device for remote authorisation enter the OTP values sent to your mobile phone \*\*\*\*\*49 and email p.\*\*\*\*\*@dga.gr". There are two input fields: "OTP via SMS" and "OTP via Email", both with green borders. A blue link "Resend OTP" is below the second field. At the bottom right, there are two buttons: "CANCEL" and "VERIFY".

d) After the Mobile RAS App is registered successfully, click “OK”

