⌂ › Docs › API Standards › PKI Management

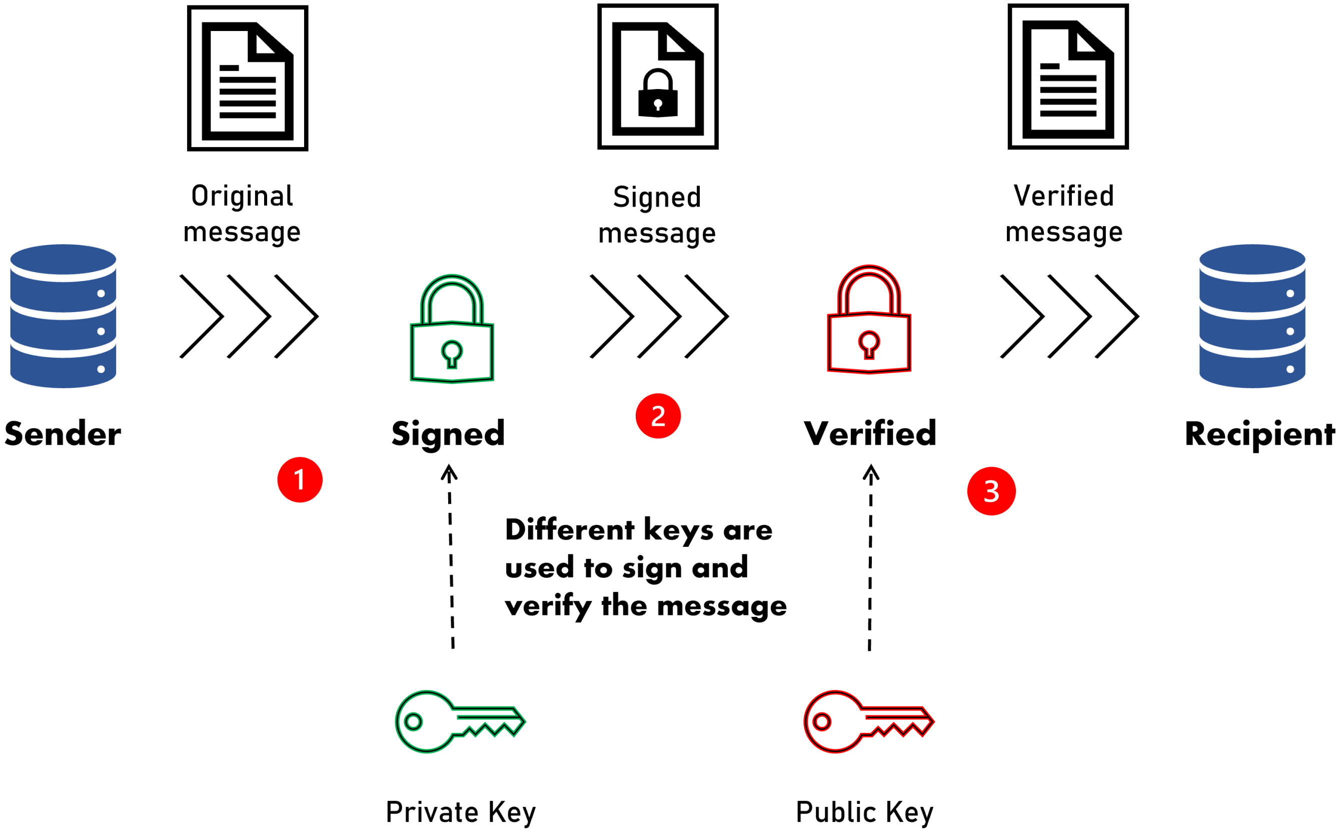
PKI Management

> **INFO**
>
> Participants are allowed to have more than one certificate/key tied to each profile and can choose which one to use for signing and verification.

The DuitNow API uses Public Key Infrastructure (PKI), which is a technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device.

The main feature of PKI is that it uses a pair of different but related keys. The key pair consists of the public key and the private key. The public key can be shared whereas the private key must be kept secret. The key pair guarantees that information encrypted with the public key can only be decrypted by the intended recipient, the holder of the private key. Conversely, when the information is encrypted with the private key and decrypted with the public key, the key pair guarantees that the information originated from a trusted source.

Refer to the PKI flow:



1. The sender signs the original message with the sender's private key.

2. The signed message is sent securely over to the recipient.

3. The signed message can only be verified by the corresponding public key before the recipient can consume the message.

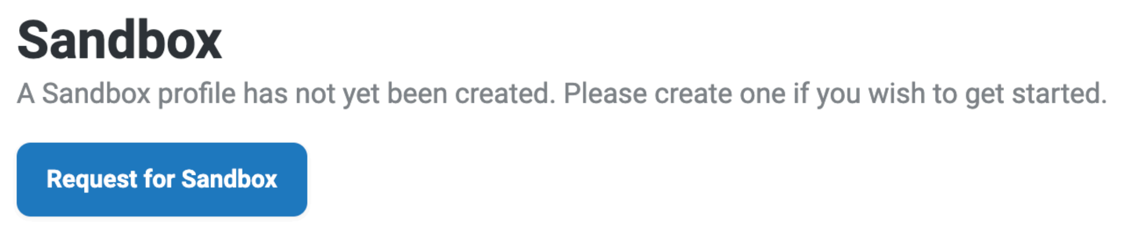
The certificate is the mechanism by which the public key is shared. A certificate is authorised by a trusted source, known as the certificate authority (CA). Participants are required to generate their own private key in RSA-SHA256 format. Once this key is generated, they will need to create a certificate to be uploaded to RPP before the API can be consumed.

Request access guide

Sandbox Production

1. Request access to the Sandbox

1. The **My Projects page** and select the **DuitNow Online Banking/Wallet Project**, Scroll to **Sandbox** section and click the button **Request for Sandbox**

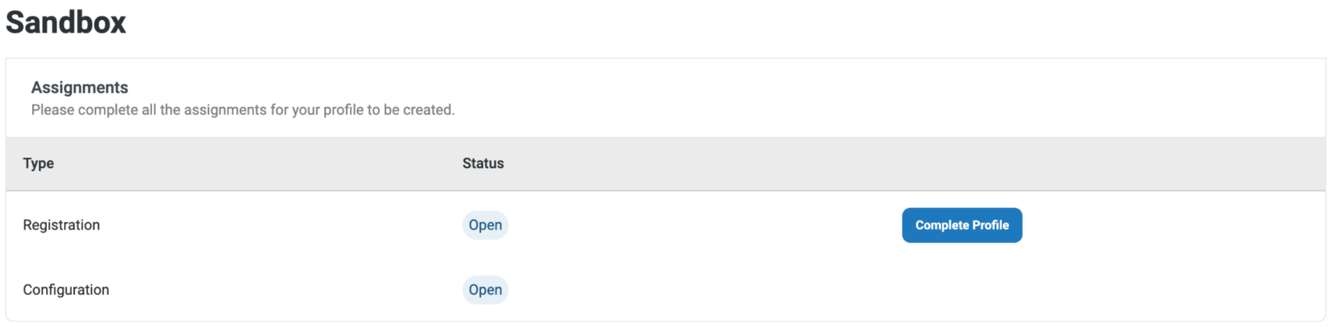


Sandbox

A Sandbox profile has not yet been created. Please create one if you wish to get started.

2. Profile registration

2.1. Click the button **"Complete Profile"** to continue the company profile registration.



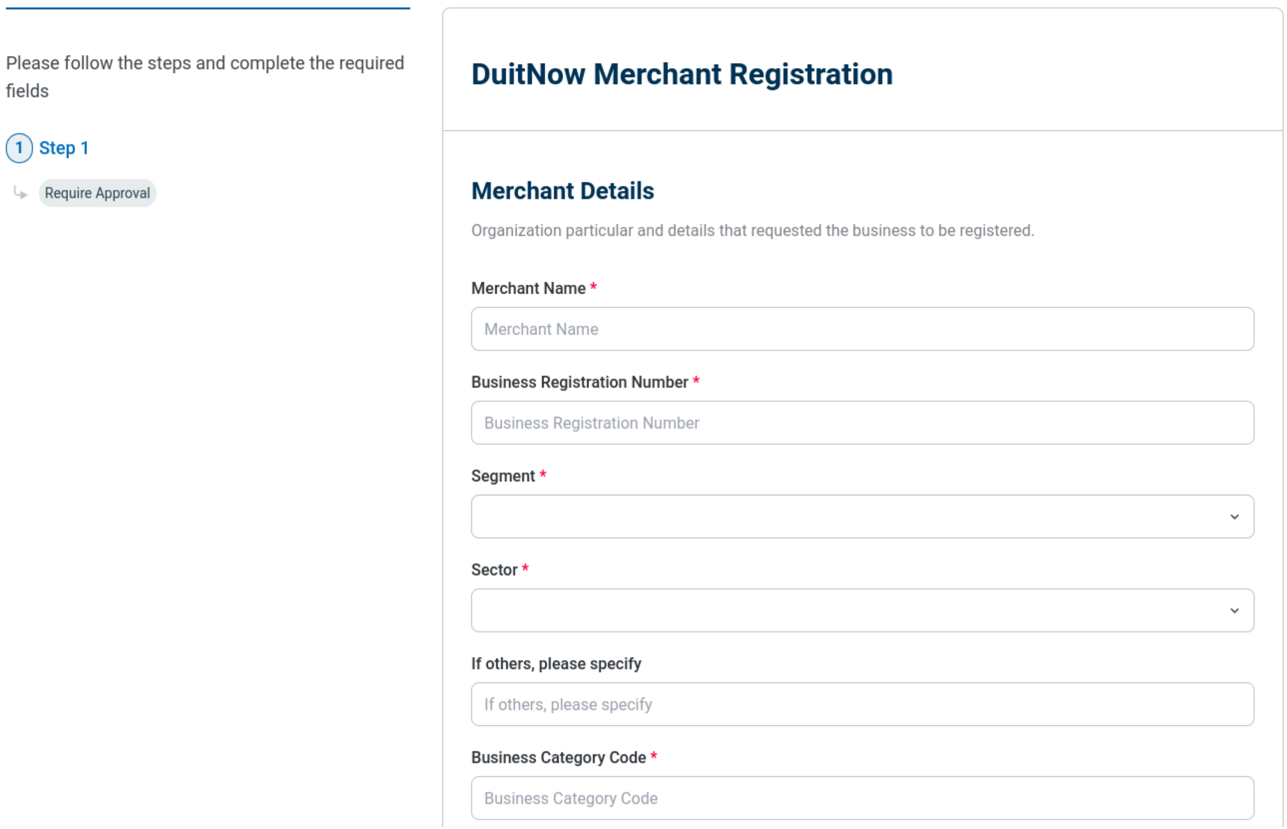
Sandbox

Assignments

Please complete all the assignments for your profile to be created.

Type	Status	
Registration	Open	Complete Profile
Configuration	Open	

2.2. Fill up your company details



Please follow the steps and complete the required fields

1 Step 1

↳ Require Approval

DuitNow Merchant Registration

Merchant Details

Organization particular and details that requested the business to be registered.

Merchant Name *

Merchant Name

Business Registration Number *

Business Registration Number

Segment *

Sector *

If others, please specify

If others, please specify

Business Category Code *

Business Category Code

How to Generate Key Pair

2.3. Generate private key and CSR (Certificate Signing Request). Using OpenSSL for Windows operation system.

```
openssl req \
      -newkey rsa:2048 -nodes -keyout example.key \
      -out example.csr
```

2.4. Generate self-signed certificate from generated CSR

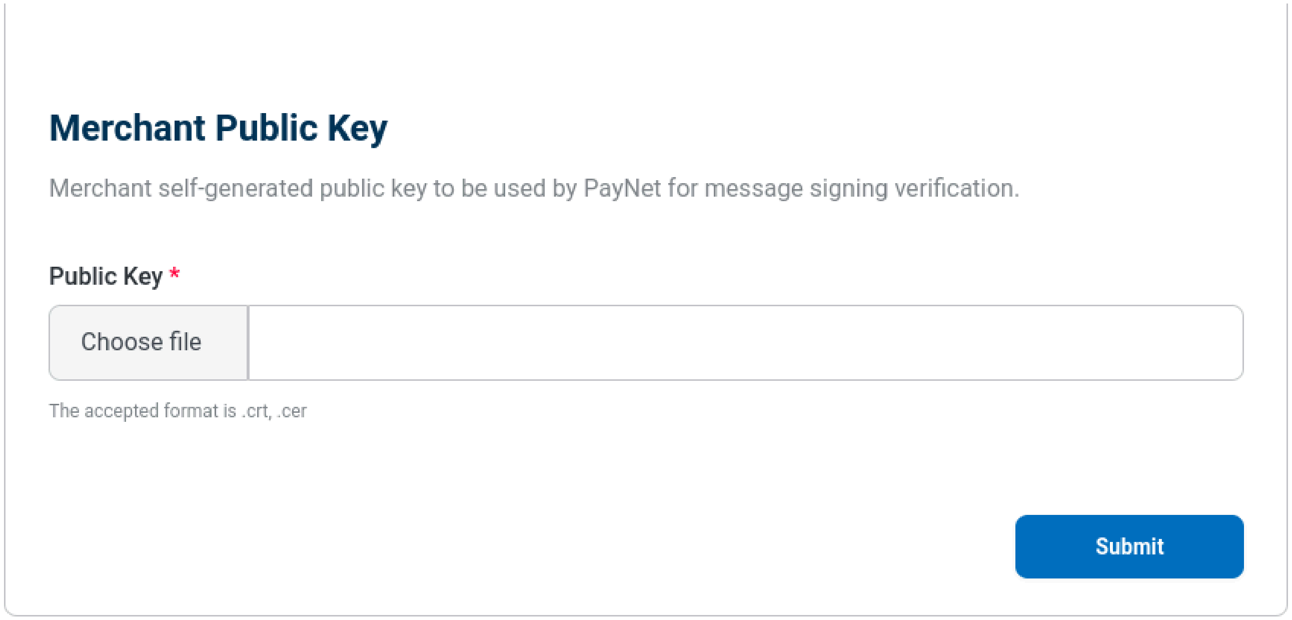
ⓘ **INFO**

For production usage, this certificate must be created by valid Certificate Authority (CA). Self-signed certificate only valid for sandbox usage.

```
openssl x509 \
       -signkey example.key \
       -in example.csr \
       -req -days 365 -out example.cer
```

Where to Upload Your Merchant Key

2.5. Use the generated CER file upload to **Public Key** field and click button **“Submit”**.



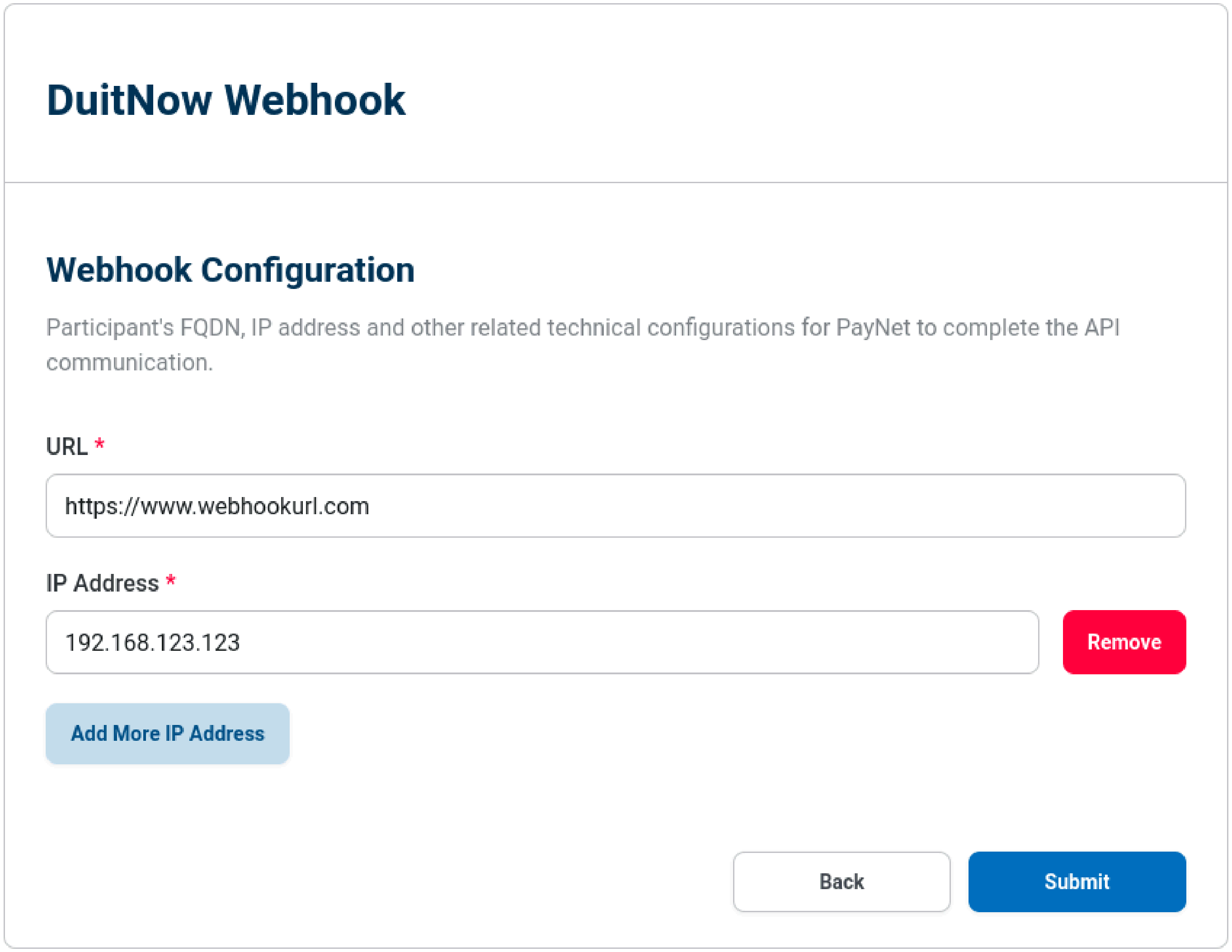
Merchant Public Key

Merchant self-generated public key to be used by PayNet for message signing verification.

Public Key *

The accepted format is .crt, .cer

2.6. Next, insert your **Webhook** and **IP address** and click button **“Submit“** to complete the registration.



DuitNow Webhook

Webhook Configuration

Participant's FQDN, IP address and other related technical configurations for PayNet to complete the API communication.

URL *

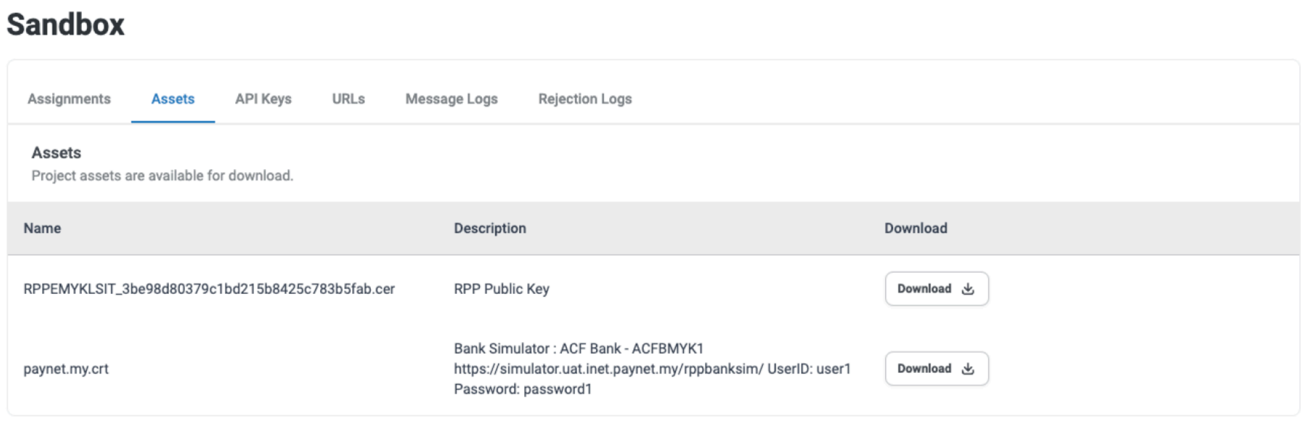
https://www.webhookurl.com

IP Address *

192.168.123.123

3. Download the Retail Payment Platform(RPP) Public Key

After approval, you will see the the **Asset** tab in the Sandbox. Click the button **“Download”** to download the RPP Public key



Sandbox

Assets

Project assets are available for download.

Name	Description	Download
RPPEMYKLSIT_3be98d80379c1bd215b8425c783b5fab.cer	RPP Public Key	Download
paynet.my.crt	Bank Simulator : ACF Bank - ACFBMYK1 https://simulator.uat.inet.paynet.my/rppbanksim/ UserID: user1 Password: password1	Download