

PKI Management

What is Public Key Infrastructure (PKI)

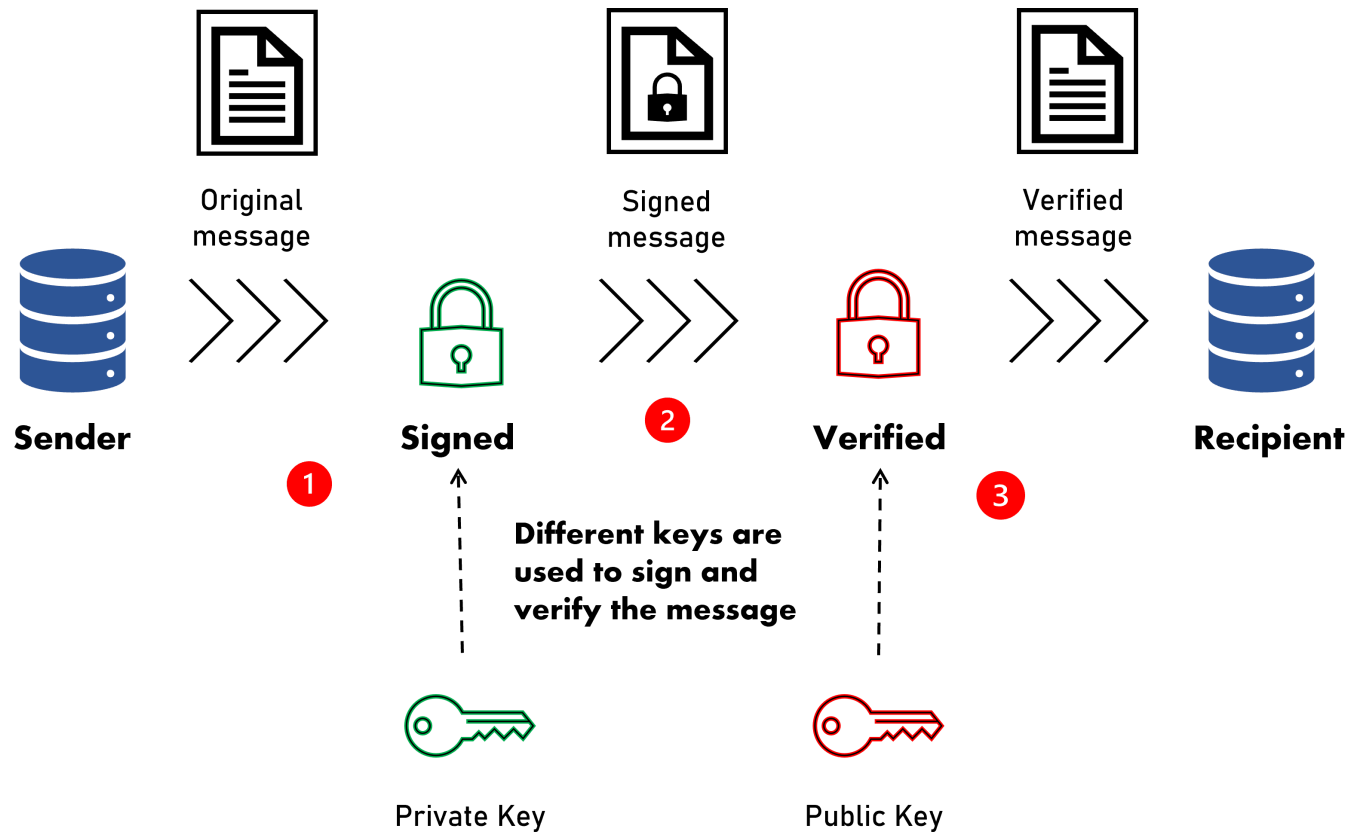
INFO

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.

How to Generate Key Pair

Using OpenSSL

Step 1: Generate private key and CSR (Certificate Signing Request)

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



Step 2: 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
```



How to Download the RPP Key

Step 1: Under the **My Projects** page, click the three dots  next to your DuitNow project and click **View project**.

My Projects

+ Create project

NAME	PRODUCT	ROLE	
Project	DuitNow	Owner	<div>...</div>

View project

Step 2: On the project page, under the relevant environment section (e.g. **Sandbox**) click the **Assets** tab.

Sandbox

Assignments

Assets

API Keys

Assignments

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

TYPE	STATUS	
Registration	Completed	<div>...</div>
Configuration	Completed	<div>...</div>

Step 3: Under the **Assets** tab, click the **Download** button next to **RPP Public Key**.

Sandbox

Assignments

Assets

API Keys

Assets

Project assets are available for download.

NAME	DESCRIPTION
uat-rpp.cer	RPP Public Key

Download

Where to Upload Your Merchant Key

Step 1: Under the **My Projects** page, click the three dots **...** next to your DuitNow project and click **View project**.

My Projects

+ Create project

NAME	PRODUCT	ROLE
Project	DuitNow	Owner

...

View project

Step 2: On the project page, under the relevant environment section (e.g. **Sandbox**) you will see a list of Assignments. Click the three dots **...** next to Registration and click **Edit profile**.

Sandbox

Assignments

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

TYPE	STATUS	
Registration	Open	<div>⋮</div>
Configuration	Open	<div>Edit profile</div>

Step 3: Under the **DuitNow Merchant Registration** tab, you will first need to fill in all the fields under **Merchant Details**, **Merchant Contact Details** and **Merchant Product Details**.

> DuitNow Merchant Registration

> DuitNow Webhook

Merchant Details

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

Merchant Name

Business Registration Number

Segment

Please select the option

Sector

Please select the option

Business Category Code

Address Line 1

Address Line 2

Then under the **Merchant Public Key** section, upload your generated public key and click the **Save** button.

