

User Guide for Sample App

Overview

This page aims to facilitate your understanding and utilization of our DuitNow Signature Generator to perform essential tasks related to signature generation, verification and JSON Web Token (JWT) creation. The Sample App features four primary tabs, each with high-level explanations of their functionalities:

1. DuitNow Version 1: Generate signatures for Version 1 using XML format.
2. DuitNow Version 2, X-Signature: Generate a signature for Version 2 using string format.
3. DuitNow Version 2, JWS: Generate a JSON Web Token (JWT).
4. Verify Signature: Verify signed messages and signatures against the public key derived from the private key used for signing.

NOTE

The sample app can be downloaded [here](#).

Getting Started

Navigate to the desired tab based on your document signing or verification needs.

Fill in the mandatory inputs as specified for each tab.

Details of the input steps for each tab explained in the respective section as below

Click the "Generate" button to obtain the desired output.

1. DuitNow Version 1 - XML


DuitNow Signature Generator

DuitNow Version 2 X-Signature

DuitNow Version 2 JWS

Verify Signature

DuitNow Version 1



Private Key Path *

Select

XML Message to sign *

Signature

Generate

Fields

Field	Definition
Private Key Path	The sender's private key file used to encrypt the information.
XML Message to sign	The original message to be signed.
Signature	The generated signed message.

Steps

- 1) User clicks the 'Select' button to search for the respective private key from their own machine for the Private Key Path.
- 2) Input the message into the XML Message to Sign field.
- 3) Click on the 'Generate' button to create the signature.

2. DuitNow Version 2 - X-Signature

 DuitNow Signature Generator

DuitNow Version 1

DuitNow Version 2 X-Signature

DuitNow Version 2 JWS

Verify Signature

**DuitNow**

Private Key Path *

Select

Business Message ID

Generate

End To End ID

Generate

Message to sign *

Signature

Generate

Fields

Field	Definition
Private Key Path	The sender's private key file used to encrypt the information.
Business Message ID	The business message Identification.
End To End ID	The transaction identification to be enquired.
Message to sign	The original message to be signed.
Signature	The generated signed message.

Steps

- 1) Click on 'Select' button to find your private key.
- 2) Click on 'Generate' button to generate the 'Business Message ID' or 'End To End ID'. A random value will be generated. Alternatively you can fill in both values with the valid format.
- 3) Once the values for 'Business Message ID' and 'End To End ID' are filled, the message signature will be generated in the 'Message to Sign' field.

NOTE

Currently, the X-signature is only used by the DuitNow TransactionEnquiry endpoint, so the generated message signature format can be referred [here](#).

- 4) If you know your 'Message to Sign' value, you can enter it without generating from the 'Business Message ID' and 'End To End ID' fields.

5) Once the mandatory values are filled, click on the 'Generate' button to create the signature.

3. DuitNow Version 2 - JWS


DuitNow Signature Generator

DuitNow Version 1

DuitNow Version 2 X-Signature

DuitNow Version 2 JWS

Verify Signature



Private Key Path *

Select

Certificate Serial Number *

Business Message ID *

Generate

JWS Payload *

JWS-Token

Generate

Fields

Field	Definition
Private Key Path	The sender's private key file used to encrypt the information.
Certificate Serial Number	Participant's Certificate Serial Number.
Business Message ID	The transaction identification to be enquired.
JWS Payload	The Original JSON data message to be signed.
JWS-Token	The generated JWT for bearer token.

Steps

- 1) Click on 'Select' button to find your private key.
- 2) Fill in your certificate serial number
- 3) Click on 'Generate' button to generate the 'Business Message ID'. A random value will be generated. Alternatively you can fill in the value with the valid format.
- 4) Fill in the JSON payload into the 'JWS Payload'. Minified and non-monified JSON message are supported.
- 5) Click on the 'Generate' button to create the JWT.

4. Verify Signature


DuitNow Signature Generator

DuitNow Version 1

DuitNow Version 2 X-Signature

DuitNow Version 2 JWS

Verify Signature



Certificate Path *

Select

Message *

Signature *

Verify Signature

Fields

Field	Definition
Certificate Path	The public key to decrypt the signed message created from the corresponding private key.
Message	The message used to sign the signature with the corresponding private key
Signature	The generated signature from the corresponding private key.

Steps

- 1) Click on 'Select' button to find your private key.
- 2) Fill in the signed message into the 'Message' field
- 3) Fill in the generated signature into the 'Signature' field.
- 3) Click on 'Verify Signature'.