

GETTING STARTED

FAQ

API OPERATIONS

Refunds

API SCHEMA

REFERENCE

DISCLAIMER

API Specification for Bangladesh Cards and Alternate Payment Methods

Version: 1.0

Description

This document introduces the **OpenAPI specification** for the REST APIs of the HSBC Collection of digital payments - HSBC Omni Collect in Bangladesh.

The target audience of this document is the Developer, Business Analyst and other related Project Team Members.

Update Log

- [Apr 27, 2022] **v1.0** Initial Version

How to Read this Document

Get to know what we offer in the [Features Overview](#) and take away the key ideas of our [API operations](#). Before you connect to our APIs, remember to collect all prerequisites and go through all requirements in the [How to Connect](#) section.

Features Overview

Checkout Solutions for Payment

You accept payments from your customers by integrating your website or app with the Hosted Payment Page serving different payment methods.

IMPORTANT NOTE:

Conditions may apply to the availability of each checkout solution and its associated payment options, please check with our support team for details.

Hosted Payment

Hosted Payment Page

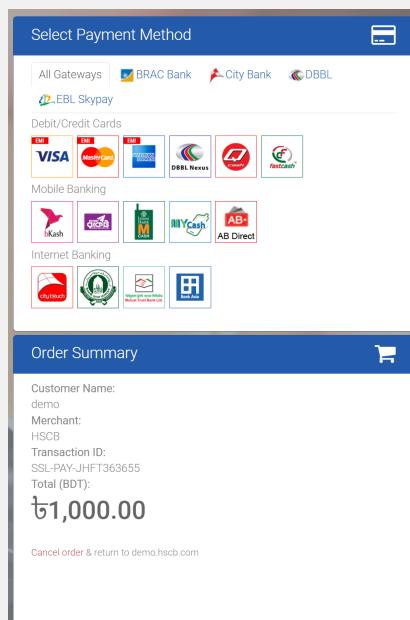
Overview The Hosted Payment Page (HPP) is a PCI DSS v3.2 compliant redirect solution, allowing you capture card data without having to worry about the PCI overhead associated with a traditional API integration.



Hosted Payment Page

- Debit / Credit Cards** - Card Data is captured securely inside HPP
- Equated Monthly Instalment (EMI)** - An option available during the Credit Card checkout process
- Internet Banking** - Redirect to Bank's Checkout page
- Mobile Banking** - Redirect to Bank's App while the checkout process is conducted on mobile device
- eWallet** - Redirect to eWallet's App while the checkout process is conducted on mobile device

Supported Payment Options



Payment Link

Integration Methods

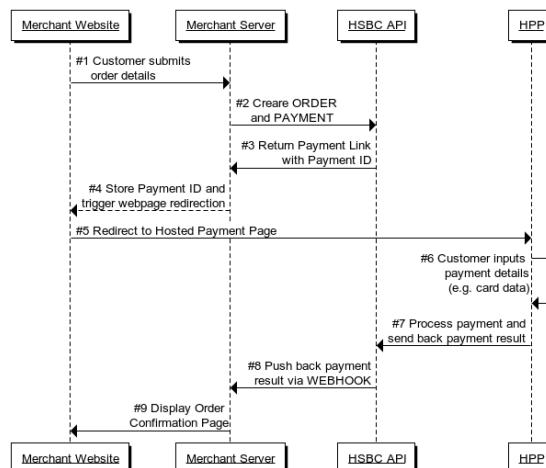
A Payment URL link you can embed directly in your website, an SMS or an email.

Recurring Payment

Easy Checkout for Recurring Payment

Overview Coming Soon, please check with our support team for details.

API Use Case of Hosted Payment Page



Please see API operations [Create Order](#), [Create Payment for an Order](#) and [Webhooks](#) for more details.

NOTE:

Merchant is recommended to store **Payment** ID to handle subsequent processes, such as [Retrieve Payment by ID](#) and [Create Refund for a Payment](#).

Refund a Payment

You can perform a full or partial refund if a payment transaction has been settled or batched. Please refer to API operation [Create Refund for a Payment](#) for more details.

Webhooks for Payment

An asynchronous callback will be pushed back to the Merchant for different payment events, such as a successful payment or a failed payment. Please refer to [Webhooks](#) for details.

INTRODUCTION
[Description](#)
[Update Log](#)
[How to Read this Document](#)
[Features Overview](#)

GETTING STARTED
[How to Connect](#)
[API Gateway URL](#)
[API Authentication](#)
[User Identification](#)
[Connection Security](#)
[Message Security](#)
[Sign & Encrypt](#)
[Decrypt & Verify](#)
[Summary](#)

[How to make API request](#)
 with Plain Message
 with Data Encryption

Data Type Overview

FAQ

[SSL Connection](#)
[Message Encryption](#)
[JOSE Framework](#)

API OPERATIONS

Orders
[Create Order](#)
[Retrieve Order by ID](#)

Payments

[Create Payment for an Order](#)
[Retrieve Payment by ID](#)
[Update a Payment](#)

Refunds

[Create Refund for a Payment](#)
[Retrieve Refund by ID](#)

Webhooks

[Payments](#)

API SCHEMA

Schema Definitions
[OrderInput](#)
[OrderOutput](#)
[Order](#)
[PaymentInput](#)
[PaymentPatch](#)
[PaymentOutput](#)
[PaymentWebhook](#)
[Payment](#)
[RefundInput](#)
[RefundOutput](#)
[Refund](#)
[Item](#)
[Card](#)
[HAL](#)
[Exception](#)
[System](#)
[Callback](#)
[Metadata](#)

REFERENCE

[Lifecycle of Cryptographic Keys](#)
[Key Generation & Exchange](#)
[Key Maintenance](#)
[Key Renewal](#)

DISCLAIMER

[Disclaimer](#)

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary
How to make API request
with Plain Message
with Data Encryption
Data Type Overview
FAQ
SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

How to Connect

API Connectivity refers to all measures and their components that establish a connection between HSBC - the API Provider and the Merchant - the API Consumer.

| | Definition | Components |
|----------------------------|---|--|
| API Authentication | HTTP BASIC Authentication | <ul style="list-style-type: none">• Username• Password |
| | Locate API Gateway Policy of the corresponding user | <ul style="list-style-type: none">• Profile ID |
| User Identification | A Merchant Profile | <ul style="list-style-type: none">• Merchant ID• Merchant Profile |
| Connection Security | HTTPS Connection (TLS 1.2) and Network Whitelisting | <ul style="list-style-type: none">• SSL Certificate• Network Whitelist |
| Message Security | Digital Signing and Data Encryption | <ul style="list-style-type: none">• A pair of Private Key & Public Key Certificate (PKI Model)• JWS Key ID• JWE Key ID |

API Gateway URL

To make API calls, you need to include this before each API endpoint.

| Production |
|---|
| https://cmb-api.hsbc.com.hk/glcm-mobilecoll-mcbd-ea-merchantservices-proxy/v1 |
| Sandbox |
| https://devclustercmb.api.p2g.net2.hsbc.com.hk/glcm-mobilecoll-mcbd-ea-merchantservices-proxy/v1 |

API Authentication

| Username & Password | | |
|-------------------------|---|--|
| Purpose | All APIs are authorized using | Basic Authorization |
| Components | <ul style="list-style-type: none">• Username• Password | |
| Where to get it? | Delivered by HSBC via secure email during onboarding procedure | |
| Implementation | In HTTP header: | Authorization: Basic [Base64-encoded Credential] |

| Profile ID | | |
|-------------------------|---|--|
| Purpose | API Gateway locates the corresponding policy of the specific API consumer | |
| Components | <ul style="list-style-type: none">• Profile ID | |
| Where to get it? | Delivered by HSBC via secure email during onboarding procedure | |
| Implementation | In HTTP header: | x-hsbc-profileid: [Profile ID] |

User Identification

| Merchant Profile & Merchant ID | | |
|--------------------------------|---|--|
| Purpose | <ul style="list-style-type: none">• Merchant Profile contains all necessary information from a Merchant in order to enable payment service.• Merchant ID is used for Merchant identification in each API call. | |



INTRODUCTION
 Description
 Update Log
 How to Read this Document
 Features Overview

GETTING STARTED

How to Connect
 API Gateway URL
 API Authentication
 User Identification
 Connection Security
 Message Security
 Sign & Encrypt
 Decrypt & Verify
 Summary

How to make API request
 with Plain Message
 with Data Encryption

Data Type Overview
 FAQ
 SSL Connection
 Message Encryption
 JOSE Framework

API OPERATIONS

Orders
 Create Order
 Retrieve Order by ID

Payments

Create Payment for an Order
 Retrieve Payment by ID
 Update a Payment

Refunds

Create Refund for a Payment
 Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions
 OrderInput
 OrderOutput
 Order
 PaymentInput
 PaymentPatch
 PaymentOutput
 PaymentWebhook
 Payment
 RefundInput
 RefundOutput
 Refund
 Item
 Card
 HAL
 Exception
 System
 Callback
 Metadata

REFERENCE

Lifecycle of Cryptographic Keys
 Key Generation & Exchange
 Key Maintenance
 Key Renewal

DISCLAIMER

Disclaimer

| Merchant Profile & Merchant ID | | |
|--------------------------------|---|--|
| Components | <ul style="list-style-type: none"> Merchant Profile | <ul style="list-style-type: none"> Merchant ID |
| Where to get it? | <ul style="list-style-type: none"> Set up by HSBC team after collect information from Merchant | <ul style="list-style-type: none"> Delivered by HSBC via secure email during onboarding procedure |
| Implementation | <i>nil</i> | <p>In HTTP header:</p> <pre>x-hsbc-msg-encrypt-id: [Merchant ID]+[JWS ID]+[JWE ID]</pre> |

Connection Security

| SSL Certificate & Network Whitelist | | |
|-------------------------------------|--|---|
| Purpose | <ul style="list-style-type: none"> Request HSBC API over HTTPS connection (TLS 1.2) | <ul style="list-style-type: none"> Accept Callback API request over HTTPS connection (TLS 1.2) |
| Components | <ul style="list-style-type: none"> Public SSL Certificate issued by HSBC | <ul style="list-style-type: none"> Merchant's web server or domain whose HTTPS connection is enabled Network Whitelist on HSBC system |
| Where to get it? | <ul style="list-style-type: none"> Downloaded automatically by Browsers or API Tools, if any problem found, please contact HSBC | <i>nil</i> <i>nil</i> |
| Implementation | <i>nil</i> | <ul style="list-style-type: none"> Merchant's domain URL will be configured in HSBC's network whitelist by HSBC team |

Message Security - Data Encryption and Signing

In addition to the Transport Layer Security, HSBC adopts additional security - Data Encryption on the message being passed across the session. This serves as a type of locked briefcase containing the data (the API message) within the HTTPS "tunnel". In other words, the communication has double protection.

DID YOU KNOW?

Javascript Object Signing and Encryption (JOSE™), is a framework that secures information transferred between parties. To achieve this, the JOSE framework provides a collection of specifications, including JSON Web Signature (JWS™) and JSON Web Encryption (JWE™).

HSBC uses [JWS](#) to sign message payloads, and [JWE](#) to encrypt the signed message. These are created by using the [Private Key & Public Key Certificate \(PKI Model\)](#).

| Private Key & Public Key Certificate (PKI Model) | | |
|--|--|--|
| Purpose | <ul style="list-style-type: none"> Digitally sign a API request message Decrypt a API response message | <ul style="list-style-type: none"> Encrypt the signed API request message Verify a signed API response message |
| Components | <ul style="list-style-type: none"> Private Key issued by Merchant | <ul style="list-style-type: none"> Public Key Certificate issued by HSBC |

GETTING STARTED

API OPERATIONS

API SCHEMA

REFERENCE

DISCLAIMER

| Private Key & Public Key Certificate (PKI Model) | | |
|--|--|--|
| Where to get it? | • Created by any Public Key Infrastructure (PKI) toolkits, such as Keytool™ and OpenSSL™. Technical detail is in here | • Exchanged with HSBC with the Public Key Certificate issued by Merchant |
| Implementation | Please see the technical detail in here | |

NOTE:
 Technically, an X.509 certificate can serve as a SSL Certificate as well as a Public Key Certificate for Data Encryption. However, for segregation of certificate usage, HSBC recommends that the Merchant uses a different X.509 Certificate for Data Encryption. Moreover, the Public Key Certificate does not have to be CA-signed. However, if the Merchant decides to enhance security, a CA-Signed Certificate is acceptable.

| keyID of JWS™ & JWE™ | | |
|----------------------|---|---|
| Purpose | • The unique identifier to bind Merchant's Private Key in order to create a JWS object - a signed Message Payload | • The unique identifier to bind HSBC's Public Key Certificate in order to create a JWE object - an encrypted JWS object |
| Components | • keyID of JWS™ | • keyID of JWE™ |
| Where to get it? | • Mutual agreed between Merchant and HSBC | |
| Implementation | Define in program coding, see demo in here | |

NOTE:
 For security purposes, [HSBC's Public Key Certificate](#) and its associated [keyID](#) is renewed every year and a Certificate Renewal process is triggered. More detail is covered in the section [Key Renewal](#)

How to Sign and Encrypt Outgoing Message

Every message sent to HSBC must be signed and encrypted. From the Merchant's perspective, an **Outgoing Message** means:

- the Request Message of a Service API, or
- the Respond Message of a Callback API.

To help you understand how to construct a Signed and Encrypted Message, let's take the Java program below as an example. Don't worry if you are not familiar with Java, the idea is to let you know the steps and the required components:

NOTE: These Java codes are for demonstration only - it's not *plug and play*.

```
private JWSObject signMessage(String messagePayload, KeyStore ks
throws UnrecoverableKeyException, KeyStoreException, NoSuchAlgorithmException
#1 Payload payload = new Payload(messagePayload);

#2 JWSHeader header = new JWSHeader
        .Builder(JWSAlgorithm.RS256)
        .keyID("0001")
        .customParam("iat", Instant.now().getEpochSecond());
#3 JWSObject jwsObject = new JWSObject(header, payload);

#4 PrivateKey privateKey = (PrivateKey) ks.getKey(keyAlias, keySelector);
#5 jwsObject.sign(signer);

    return jwsObject;
}
```

1. Prepare your **Message Payload**, that is, the plain [json](#) request message.
2. Create a **JWS Header** where the parameters are as follows:

```
{
    "alg": "RS256",      //Signing Algorithm is RS256
    "kid": "0001",       //Put your own Key ID value, "0001" is just an example
    "iat": "1625587913" //Issued At - the time this request is made
}
```

3. Create a **JWS Object** by combining JWS Header and Message Payload.
4. Retrieve your **Private Key** as the signer.
5. Create a **Signed JWS Object** by signing it with the Private Key.

```

private JWEObject getEncryptedJWEObject(JWSObject jwsObject, RS
throws JOSEException {
#1 Payload jwepayload = new Payload(jwsObject.serialize());
#2 JWEHeader jweheader = new JWEHeader.Builder(JWEAlgorithm.RS
#3 JWEObject jweObject = new JWEObject(jweheader, jwepayload);
#4 JWEEncrypter encrypter = new RSAEncrypter(key);
#5 jweObject.encrypt(encrypter);

    return jweObject;
}

```

1. Prepare your **JWE Payload**, that is, the **Signed JWS Object**.
2. Create the **JWE Header**. The algorithm used to encrypt the message body is **A128GCM** while the algorithm used to encrypt the encryption key is **RSA_OAEP_256**. **JWE keyID** is **0002**.
3. Create the **JWE Object** by combining JWE Header and JWE Payload.
4. Retrieve the **HSBC's Public Key** as the encrypter.
5. Create the **Encrypted JWE Object** by encrypting it with HSBC's Public Key.

You are now ready to put the Encrypted JWE Object in the message body (*you may need to first serialize it into String format, depends on your program code design*) of any API call.

How to Decrypt Message and Verify Signature of an Incoming Message

Every message sent from HSBC must be decrypted and verified. From the Merchant's perspective, an **Incoming Message** means:

- the Respond Message of a Service API, or
- the Request Message of a Callback API.

Let's look into the following example to see how to decrypt a response message from HSBC:

```

private String decryptMessage(String respMsgPayload, KeyStoreFa
throws KeyStoreException, NoSuchAlgorithmException, Certifica
java.text.ParseException, UnrecoverableKeyException, J
#1 JWEObject jweObject = JWEObject.parse(respMsgPayload);

#2 PrivateKey privateKey = (PrivateKey) keyStore.getPrivateKey

#3 JWEDecrypter decrypter = new RSAEncrypter(privateKey);
#4 String signedMessage = jweObject.getPayload().toString();
    return signedMessage;
}

```

1. Create an **Encrypted JWE Object** by parsing the encrypted response message payload.
2. Retrieve the **Private Key** as the decrypter.
3. Decrypt the JWE Object using your Private Key.
4. Get the **Signed Message** from the decrypted JWE Object.

You are now able to extract the plain **json** message, but first you **must verify** the signature to guarantee data integrity.

```

private String verifySignature(String signedMessage, KeyStore k
throws KeyStoreException, JOSEException, ParseException {
#1 JWSObject jwsObject = JWSObject.parse(signedMessage);

    Certificate certificate = ks.getCertificate(keyAlias);
#2 JWSVerifier verifier = new RSASSAVerifier((RSAPublicKey) ce
#3 if (!jwsObject.verify(verifier)) {
        throw new ValidationException("Invalid Signature");
    }
#4 return jwsObject.getPayload().toString();
}

```

1. Create a **JWS Object** by parsing the **Signed Message**.
2. Retrieve the **HSBC's Public Key** as the verifier.
3. Verify the signed JWS Object. Invoke error handling if an invalid signature is found (*depends on your code design*).
4. Get the plain **json** message for further actions.

Summary

| Components \ Steps | Message Signing | Message Encryption | Message Decryption | Verify Signature |
|--------------------|-----------------------------|--------------------|--------------------|------------------|
| JWS Object | Signing Algorithm: RS256 | | | |

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED
How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption
Data Type Overview
FAQ
SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS
Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID
Webhooks
Payments

API SCHEMA
Schema Definitions
OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE
Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER
Disclaimer

| Components \ Steps | Message Signing | Message Encryption | Message Decryption | Verify Signature |
|------------------------|-------------------|---|--------------------|------------------|
| JWE Object | | JWE Algorithm: <code>RSA_OAEP_256</code> | | |
| KeyID | <code>0002</code> | <code>0002</code> | | |
| Merchant's Private Key | Used as Signer | Encryption Method: <code>A128GCM</code> | Used as Decrypter | |
| HSBC's Public Key | | Used as Encrypter | | Used as Verifier |

How to Make an API Request

An API request can be submitted without Message Encryption, in case you want to:

- learn about the basic API Call;
- test API connectivity before spending substantial development effort on Message Encryption.

Data encryption is a required data security imposed by HSBC standards. The Merchant has to invoke the encryption logic before moving to Production and must be fully tested during the testing phase.

Make Your API Request with Plain Messages

NOTE:
In the Sandbox Environment you can skip message encryption.
However, this is for testing purpose only.

Submit an example API request using cURL™

cURL™ is a simple command-line tool that enables you to make any HTTP request. Merchant can choose any other GUI tool such as Postman™ and SoapUI™.

Step 1. Run this command on your platform:

POST

```
#1 curl -X POST "https://devclustercmb.api.p2g.netd2.hsbc.c
#2 -H "message_encrypt: false"
#3 -H "Authorization: Basic ew91cl91c2VybmcftTp5b3vyX3Bhc3
#4 -H "x-HSBC-profileid: 8b915a4f5b5047f091f210e2232b5ced"
#5 -H "x-HSBC-msg-encrypt-id: 42298549900001+0001+0002"
#6 -H "Content-Type: application/json"
#7 -d "[ {"txRef": "PAY-QJZV956664", "merId": "42298549900001+0001+0002"} ]"
```

1. Submit the `POST` request to the API URL endpoint.
2. Set the secret header `message_encrypt: false` to indicate this API request is without message encryption. This header is only applicable in Sandbox environment.
3. Put the `Basic Authorization` in HTTP header `Authorization`.
4. Put the `Profile ID` in HTTP header `x-HSBC-profileid`.
5. Put the `Merchant ID`, the `JWS ID` and the `JWE ID` in HTTP header `x-HSBC-msg-encrypt-id` respectively.
6. Set the `Content-Type` to JSON format.
7. Plain `json` message payload.

GET

```
#1 curl -X GET "https://devclustercmb.api.p2g.netd2.hsbc.c
#2 -H "message_encrypt: false"
#3 -H "Authorization: Basic ew91cl91c2VybmcftTp5b3vyX3Bhc3
#4 -H "x-HSBC-profileid: 8b915a4f5b5047f091f210e2232b5ced"
#5 -H "x-HSBC-msg-encrypt-id: 42298549900001+0001+0002"
#6 -H "Content-Type: application/json"
```

1. Submit the `GET` request to the API URL endpoint.
2. Set the secret header `message_encrypt: false` to indicate this API request is without message encryption. This header is only applicable in Sandbox environment.
3. Put the `Basic Authorization` in HTTP header `Authorization`.
4. Put the `Profile ID` in HTTP header `x-HSBC-profileid`.

5. Put the **Merchant ID**, the **JWS ID** and the **JWE ID** in HTTP header **x-HSBC-msg-encrypt-id** respectively.
6. Set **Content-Type** to JSON format.

Step 2. Receive the response message in plain **json** format.

Making API Request with Message Encryption

Step 1. Run this cURL™ command on your platform:

POST

```
#1 curl -X POST "https://devclustercmb.api.p2g.netd2.hsbc.c
#2 -H "Authorization: Basic ew91c191c2VybmcFzTpb3yX3Bhc3
#3 -H "x-HSBC-profileid: 8b915a4f5b5047f091f210e2232b5ced"
#4 -H "x-HSBC-msg-encrypt-id: 4229854990001+0001+0002"
#5 -H "Content-Type: application/json"
#6 -d "eyJraWQiOiIwMDAxIiwjIjoiQTEyOEdDTIsImFsZyI6IlJ
```

1. Submit the **POST** request to the API URL endpoint. Any **{id}** adhered in the URL must be encrypted.
2. Put the **Basic Authorization** in HTTP header **Authorization**.
3. Put the **Profile ID** in HTTP header **x-HSBC-profileid**.
4. Put the **Merchant ID**, the **JWS ID** and the **JWE ID** in HTTP header **x-HSBC-msg-encrypt-id** respectively.
5. Set the **Content-Type** to JSON format.
6. The Encrypted Message Payload.

GET

```
#1 curl -X GET "https://devclustercmb.api.p2g.netd2.hsbc.co
#2 -H "Authorization: Basic ew91c191c2VybmcFzTpb3yX3Bhc3
#3 -H "x-HSBC-profileid: 8b915a4f5b5047f091f210e2232b5ced"
#4 -H "x-HSBC-msg-encrypt-id: 4229854990001+0001+0002"
#5 -H "Content-Type: application/json"
```

1. Submit the **GET** request to the API URL endpoint. Any **{id}** adhered in the URL must be encrypted.
2. Put the **Basic Authorization** in HTTP header **Authorization**.
3. Put the **Profile ID** in HTTP header **x-HSBC-profileid**.
4. Put the **Merchant ID**, the **JWS ID** and the **JWE ID** in HTTP header **x-HSBC-msg-encrypt-id** respectively.
5. Set the **Content-Type** to JSON format.

! NOTE:

Data Encryption invokes compulsory prerequisites, such as **JOSE library** and program coding, please make sure the section on **Message Security** has been gone through thoroughly.

Step 2. For a successful request (HTTP Status Code 200), an encrypted response message is returned, otherwise, a plain **json** with failure message is returned.

Data Type Overview

Data Type Control:

| Data Type | Allowed Characters | Definition & Important Notice |
|--------------------------------|-----------------------------|--|
| String (For general field) | Alphanumeric and Symbols | General field means field which is NOT a critical field. HSBC system will execute characters checking upon all string fields we received in order to tackle security vulnerability, such as Cross-site Scripting. Yet, we recommend you to try use Alphanumeric only for most cases. |
| String (For critical field) | 0-9 a-z A-Z - _ | Critical field is used to be either a key or search criteria in HSBC backend system and hence tight restriction is applied to the allowed characters. Moreover, the starting and ending space of the string value will be trimmed before stored in HSBC system. For example, string " <code>example 12 34</code> " will be trimmed to " <code>example 12 34</code> ". |

List of Critical Fields:
All **id** (s)

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED
How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview

FAQ

SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

| Data Type | Allowed Characters | Definition & Important Notice |
|-----------|--------------------|---|
| Integer | 0-9 | Instead of having Max Length check for String, integer range will be checked, e.g. 0 ≤ x ≤ 9999 |

Field Mandatory Control:

| Field Type | Mandatory | Definition & Important Notice |
|------------|-------------|---|
| | Mandatory | Annotated with required tag in field definition section. |
| | Optional | Field & value must be present in the request with valid JSON format. |
| | Conditional | Annotated with optional tag in field definition section. |
| | | If you don't want to pass fields that are optional, your handler should not pass neither empty strings <code>{"example": ""}</code> nor blank value <code>{"example": " "}</code> . |
| | | Annotated with conditional tag in field definition section. |
| | | Required under a specific condition whose logic is always provided in the field definition if it is a Conditional Field. |

Time Zone Control:

| Aspect | Format | Definition & Important Notice |
|---------------------|--|--|
| In Request Message | <code>yyyy-MM-dd'T'HH:mm:ssZ</code> | Time zone is expected to be GMT+8 (Malaysia standard time). Merchant is required to perform any necessary time zone conversion before submit request if needed. |
| In Response Message | <code>yyyy-MM-dd'T'HH:mm:ss±hh:mm</code> | Timezone returned in <code>api_gw</code> object is generated from HSBC API Gateway which located in Cloud and hence is calculated in GMT+0 . On the other hand, time field in <code>response</code> object will be returned together with timezone information. For more details, please read each field definition carefully. |

FAQ

SSL Connection Questions

Where can I find the HSBC SSL server certificates?

The Merchant developer can export SSL server certificates installed in your browser. To achieve this, visit the domain of the corresponding API endpoint in your browser. For example, to get the SSL certificate of sandbox environment, use the domain name <https://devclustercmb.api.p2g.netd2.hsbc.com.hk/>

However, in production, we provide a certificate and require TLS 1.2 implementation.

Message Encryption Questions

What certificates do I need to work with Message Encryption in HSBC's sandbox and production environments?

A self-sign certificate is acceptable. However, if the Merchant decides to enhance security, a CA-Signed Certificate is also acceptable.

Javascript Object Signing and Encryption (JOSE) Framework Questions

Where can I get more information about JOSE Framework?

If you want to fully understand the framework, you can read [here](#) for more details.

Please note these urls or websites do not belong to HSBC, use them at your own discretion. By clicking these urls or websites signifies you accept these terms and

conditions.

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

Where can I download JOSE libraries for development?

For your reference, you may find the following JOSE libraries of different programming languages.

- Ruby
- Python
- PHP
- Java
- Node
- .NET

Please note these urls or websites do not belong to HSBC, use them at your own discretion. By clicking these urls or websites signifies you accept these terms and conditions.

Orders

Create Orders and link them to [Payments](#). Order creation is the first and an important step as it helps you associate every payment with an order. Orders and payments can be created in one-go or separately.

Orders

Create an Order

POST /orders

DESCRIPTION

This endpoint creates an Order.

To facilitate the checkout process of an e-commerce sale, this endpoint can offer a faster way to create [Order](#) and [Payment](#) in one-go by expanding the API operation to multiple entities. Please see the details as follows.

Nevertheless, merchant can still choose to create [Order](#) and [Payment](#) separately which may fit more on some other use cases such as bill payment or bulk processing.

REQUEST PARAMETERS

Authorization BASIC [Base64-encoded Credential]

required
in header

x-hsbc-profileid [Profile ID]

required
in header

x-hsbc-msg-encrypt-id [Merchant ID]+[JWS ID]+[JWE ID]

required
in header

Content-Type application/json

required
in header

\$expand: string[] in query

The \$expand system query option specifies the related resources to be included in line with the original resource.

Available Value: payment

POST /orders?\$expand=payment

Use Case: Create objects [Order](#) and [Payment](#) in one go. This is recommended for easing the no. of API calls.

How-to: Include [Payment](#) object in the request body

POST /orders

Use Case: Only [Order](#) will be created. This gives the flexibility to link to a [Payment](#) object at a later time

How-to: Exclude [Payment](#) object in the request body. After an [Order](#) is created, create [Payment](#) and link [Order](#) by [POST /orders/{id}/payment](#)

REQUEST BODY

Request Content-Types: application/json

Request Example

Submit without Payment

```
{  
  "txn_reference": "ORDER-1234QWER",  
  "amount": 1000,  
  "currency": "BDT",  
  "description": "Order Description",  
  "items": [  
    {  
      "product_name": "Product Item 1",  
      "product_id": "A",  
      "unitAmt": 900,  
      "unit": 1,  
      "vat": 100,  
      "subAmt": 1000  
    }  
,  
    "metadata": {  
      "note_1": "Customer is a VIP",  
      "note_2": "In-store credit is used"  
    }  
  ]  
}
```

Submit with Hosted Payment

```
{  
  "txn_reference": "ORDER-1234QWER",  
  "amount": 1000,  
  "currency": "BDT",  
  "description": "Order Description",  
  "items": [  
    {  
      "product_name": "Product Item 1",  
      "product_id": "A",  
      "unitAmt": 900,  
      "unit": 1,  
      "vat": 100,  
      "subAmt": 1000  
    }  
,  
    "metadata": {  
      "note_1": "Customer is a VIP",  
      "note_2": "In-store credit is used"  
    },  
    "payment": {  
      "payment_method": {  
        "hosted_payment": {  
          "url_settings": {  
            "return_page": {  
              "url": "https://www.example.com/return"  
            }  
          }  
        }  
      }  
    }  
  ]  
}
```



OrderInput

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

OrderInput

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

```
"success": "https://merchant.com/returnPageSuccess",
"fail": "https://merchant.com/returnPageFail",
"cancel": "https://merchant.com/returnPageCancel"
},
"notification": "https://merchant.com/returnStatus"
},
"card_option": [
"city_visa",
"bankasia"
],
"billing": {
"first_name": "khana",
"last_name": "riphata",
"email": "khana.riphata@sekha.com",
"phone": "01054 694200",
"street1": "71 Dit Road, 4th Floor",
"street2": "Malibagh Chowdhury Para",
"city": "Dhaka",
"state": "Dhaka",
"postal_code": "n/a",
"country": "Bangladesh"
}
}
}
}
```

RESPONSES

200 OK

Successful operation.

OrderOutput

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

400 Bad Request

Exception

Missing or invalid Parameters.

403 Forbidden

Authorization credentials are missing or invalid.

404 Not Found

Empty resource/resource not found.

500 Internal Server Error

The request failed due to an internal error.

Response Content-Types: application/json

Response Example (200 OK)

Submit without Payment

```
{
"system": {
"messageId": "89817674-da00-4883",
"resultCode": "200",
"returnReason": "Successful operation",
"sentTime": "2016-11-15T10:00:00.000Z",
"responseTime": "2016-11-15T10:00:00.000Z"
},
"response": {
"order": {
"id": "ORDER-1234QWER",
"txn_reference": "ORDER-1234QWER",
"created_at": "2021-06-11T12:10:25Z",
"last_modified": null,
"amount": 1000,
"currency": "BDT",
"description": "Order Description",
"items": [
{
"product_name": "Product Item 1",
"product_id": "A",
"unitAmt": 900,
"unit": 1,
"vat": 100,
"subAmt": 1000
}
],
"metadata": {
"note_1": "Customer is a VIP",
"note_2": "In-store credit is used"
},
"links": [
{
"href": "/orders/@order_id",
"id": {
"order_id": "ORDER-1234QWER"
},
"rel": "self",
"method": "GET"
},
{
"href": "/orders/@order_id/payment",
"id": {
"order_id": "ORDER-1234QWER"
},
"rel": "payment",
"method": "POST"
}
]
}
}
```

Submit with Hosted Payment

```
{
"system": {
"messageId": "89817674-da00-4883",
"resultCode": "200",
"returnReason": "Successful operation",
"sentTime": "2016-11-15T10:00:00.000Z",
"responseTime": "2016-11-15T10:00:00.000Z"
},
"response": {
"order": {
"id": "ORDER-1234QWER",
"txn_reference": "ORDER-1234QWER",
"created_at": "2021-06-11T12:10:25Z",
"last_modified": null,
"amount": 1000,
"currency": "BDT",
"description": "Order Description",
"items": [
{
"product_name": "Product Item 1",
"product_id": "A",
"unitAmt": 900,
"unit": 1,
"vat": 100,
"subAmt": 1000
}
]
```

```

    "vat": 100,
    "subAmt": 1000
  },
  "metadata": {
    "note_1": "Customer is a VIP",
    "note_2": "In-store credit is used"
  },
  "payments": [
    {
      "id": "PAYMENT-5678TYUI",
      "bank_tran_id": null,
      "created_at": "2021-06-11T12:10:25Z",
      "last_modified": null,
      "amount": null,
      "store_amount": null,
      "currency": null,
      "status": "PENDING",
      "payment_method": {
        "hosted_payment": {
          "access_method": {
            "payment_link": "https://pay.sandbox.realexpayments.com/card.html?guid=f82dc878-4752-4d25-8c4b-7d4803a863ec"
          },
          "url_settings": {
            "return_page": {
              "success": "https://merchant.com/returnPageSuccess",
              "fail": "https://merchant.com/returnPageFail",
              "cancel": "https://merchant.com/returnPageCancel"
            },
            "notification": "https://merchant.com/returnStatus"
          }
        },
        "card_option": [
          "city_visa",
          "bankasia"
        ],
        "payment_option": null,
        "billing": {
          "first_name": "khana",
          "last_name": "riphata",
          "email": "khana.riphata@sekha.com",
          "phone": "01054 694200",
          "street1": "71 Dit Road, 4th Floor",
          "street2": "Malibagh Chowdhury Para",
          "city": "Dhaka",
          "state": "Dhaka",
          "postal_code": "n/a",
          "country": "Bangladesh"
        }
      }
    },
    "metadata": null,
    "links": [
      {
        "href": "/payments/@payment_id",
        "id": {
          "payment_id": "PAYMENT-5678TYUI"
        },
        "rel": "self",
        "method": "GET"
      },
      {
        "href": "/payments/@payment_id",
        "id": {
          "payment_id": "PAYMENT-5678TYUI"
        },
        "rel": "update",
        "method": "PATCH"
      }
    ]
  ],
  "links": [
    {
      "href": "/orders/@order_id",
      "id": {
        "order_id": "ORDER-1234QWER"
      },
      "rel": "self",
      "method": "GET"
    }
  ]
}

```

Response Example (400 Bad Request)

```

{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "400",
    "returnReason": "<Corresponding Error Message>",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "request_result": {
      "api_gateway": {
        "code": "999999",
        "message": "System Error"
      },
      "payment_gateway": {
        "code": null,
        "message": "FAILED"
      }
    }
  }
}

```

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

Retrieve a particular Order by ID

GET /orders/{id}

DESCRIPTION

This endpoint retrieves the details of a particular Order.

Retrieval of other related-objects such as Payment and Refund in one single action is possible by expanding the API operation to multiple entities. This can benefit merchant by reducing the number of API calls. However, it may hit performance issue if one particular Order associates a long list of Payments or Refunds, so please choose to use this feature wisely.

REQUEST PARAMETERS

Authorization BASIC [Base64-encoded Credential]

required
in header

x-hsbc-profileid [Profile ID]

required
in header

x-hsbc-msg-encrypt-id [Merchant ID]+[JWS ID]+[JWE ID]

required
in header

Content-Type application/json

required
in header

id: string Unique **id** of **order**

required
in path

Data Encryption is enforced.

\$expand: string[] in query

The **\$expand** system query option specifies the related resources to be included in line with the original resource.

Available Values: **payment** **refund**

GET /orders/{id}

Only **Order** will be returned in response, all other related-objects will be associated in **links**

GET /orders/{id}?\$expand=payment

Order and **Payment** will be returned in response, all other related-objects will be associated in **links**

GET /orders/{id}?
\$expand=payment/refund

Order, **Payment** and **Refund** will be returned in response

RESPONSES

200 OK

OrderOutput

Successful operation.

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

400 Bad Request

Exception

Missing or invalid Parameters.

403 Forbidden

Authorization credentials are missing or invalid.

404 Not Found

Empty resource/resource not found.

500 Internal Server Error

The request failed due to an internal error.

Response Content-Types: application/json

Response Example (200 OK)

Order only

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "200",
    "returnReason": "Successful operation",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "order": {
      "id": "ORDER-12340WER",
      "txnid": "ORDER-12340WER",
      "created_at": "2021-06-11T12:10:25Z",
      "last_modified": null,
      "amount": 1000,
      "currency": "BDT",
      "description": "Order Description",
      "items": [
        {
          "product_name": "Product Item 1",
          "product_id": "A",
          "unitAmt": 900,
          "unit": 1,
          "vat": 100,
          "subAmt": 1000
        }
      ],
      "metadata": {
        "note_1": "Customer is a VIP",
        "note_2": "In-store credit is used"
      }
    }
  }
}
```

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

```
    "links": [
      {
        "href": "/payments/@payment_id",
        "id": {
          "payment_id": "PAYMENT-5678TYUI"
        },
        "rel": "payment",
        "method": "GET"
      }
    ]
  }
}
```

Order + Payment

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "200",
    "returnReason": "Successful operation",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "order": {
      "id": "ORDER-1234QWER",
      "txn_reference": "ORDER-1234QWER",
      "created_at": "2021-06-11T12:10:25Z",
      "last_modified": null,
      "amount": 1000,
      "currency": "BDT",
      "description": "Order Description",
      "items": [
        {
          "product_name": "Product Item 1",
          "product_id": "prod-9ijn8uhb",
          "unitAmt": 900,
          "unit": 1,
          "vat": 100,
          "subAmt": 1000
        }
      ],
      "metadata": null,
      "payments": [
        {
          "id": "PAYMENT-5678TYUI",
          "bank_tran_id": "PAYMENT-5678TYUI",
          "created_at": "2021-06-11T14:10:25Z",
          "last_modified": "2021-06-12T14:10:25Z",
          "amount": 1000,
          "store_amount": 975,
          "currency": "BDT",
          "status": "VALID",
          "payment_method": {
            "hosted_payment": {
              "access_method": {
                "payment_link": "https://pay.sandbox.realexpayments.com/card.html?guid=f82dc878-4752-4d25-8c4b-7d48b3a863ec"
              }
            },
            "url_settings": {
              "return_page": {
                "success": "https://merchant.com/returnPageSuccess",
                "fail": "https://merchant.com/returnPageFail",
                "cancel": "https://merchant.com/returnPageCancel"
              },
              "notification": "https://merchant.com/returnStatus"
            }
          },
          "card_option": [
            "city_visa",
            "bankasia"
          ],
          "payment_option": "CARD",
          "billing": {
            "first_name": "khana",
            "last_name": "riphata",
            "email": "khana.riphata@sekha.com",
            "phone": "+01954 694200",
            "street1": "71 Dic Road, 4th Floor",
            "street2": "Malibagh Chowdhury Para",
            "city": "Dhaka",
            "state": "Dhaka",
            "postal_code": "n/a",
            "country": "Bangladesh"
          },
          "card": {
            "brand": "VISA-City Bank",
            "issuer": "TRUST BANK, LTD.",
            "mcn": "418117XXXXXX6675"
          }
        }
      ],
      "metadata": null,
      "links": [
        {
          "href": "/payments/@payment_id",
          "id": {
            "payment_id": "PAYMENT-5678TYUI"
          },
          "rel": "self",
          "method": "GET"
        },
        {
          "href": "/payments/@payment_id",
          "id": {
            "payment_id": "PAYMENT-5678TYUI"
          },
          "rel": "update",
          "method": "PATCH"
        },
        {
          "href": "/refunds/@refund_id",
          "id": {
            "refund_id": "6141afffc4a2ea"
          },
          "rel": "refund",
          "method": "GET"
        }
      ]
    }
  }
}
```



INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

```
{
  "links": [
    {
      "href": "/payments/@payment_id/refund",
      "id": {
        "payment_id": "PAYMENT-5678TYUI"
      },
      "rel": "refund",
      "method": "POST"
    }
  ],
  "links": null
}
```

Order + Payment + Refund

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "200",
    "returnReason": "Successful operation",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "order": {
      "id": "ORDER-12340WER",
      "txnid": "ORDER-12340WER",
      "created_at": "2021-06-11T12:10:25Z",
      "last_modified": null,
      "amount": 1000,
      "currency": "BDT",
      "description": "Order Description",
      "items": [
        {
          "product_name": "Product Item 1",
          "product_id": "prod_9ijn8uhb",
          "unitAmt": 900,
          "unit": 1,
          "vat": 100,
          "subAmt": 1000
        }
      ],
      "metadata": null,
      "payments": [
        {
          "id": "PAYMENT-5678TYUI",
          "bank_tran_id": "PAYMENT-5678TYUI",
          "created_at": "2021-06-11T14:10:25Z",
          "last_modified": "2021-06-12T14:10:25Z",
          "amount": 1000,
          "store_amount": 975,
          "currency": "BDT",
          "status": "VALID",
          "payment_method": {
            "hosted_payment": {
              "access_method": [
                "payment_link": "https://pay.sandbox.reallexpayments.com/card.html?guid=f82dc878-4752-4d25-8c4b-7d48b3a863ec"
              ],
              "url_settings": {
                "return_page": {
                  "success": "https://merchant.com/returnPageSuccess",
                  "fail": "https://merchant.com/returnPageFail",
                  "cancel": "https://merchant.com/returnPageCancel"
                },
                "notification": "https://merchant.com/returnStatus"
              },
              "card_option": [
                "city_visa",
                "bankasia"
              ],
              "payment_option": "CARD",
              "billing": {
                "first_name": "khana",
                "last_name": "riphata",
                "email": "khana.riphata@sekha.com",
                "phone": "01054 694200",
                "street1": "71 Dhr Road, 4th Floor",
                "street2": "Malibagh Chowdhury Para",
                "city": "Dhaka",
                "state": "Dhaka",
                "postal_code": "n/a",
                "country": "Bangladesh"
              },
              "card": {
                "brand": "VISA-City Bank",
                "issuer": "TRUST BANK, LTD.",
                "mcn": "418117XXXXXX6675"
              }
            }
          },
          "metadata": null,
          "refunds": [
            {
              "id": "6141afffc4a2ea",
              "refund_ref_id": "6141afffc4a2ea",
              "created_at": "2021-06-11T14:10:25Z",
              "last_modified": "2021-06-12T14:10:25Z",
              "amount": 1000,
              "currency": "BDT",
              "status": "pending",
              "metadata": null,
              "links": [
                {
                  "href": "/refunds/@refund_id",
                  "id": {
                    "refund_id": "6141afffc4a2ea"
                  },
                  "rel": "self",
                  "method": "GET"
                }
              ]
            }
          ]
        }
      ]
    }
  }
}
```

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview

FAQ

SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

```
"links": [
  {
    "href": "/payments/@payment_id",
    "id": {
      "payment_id": "PAYMENT-5678TYUI"
    },
    "rel": "self",
    "method": "GET"
  },
  {
    "href": "/payments/@payment_id",
    "id": {
      "payment_id": "PAYMENT-5678TYUI"
    },
    "rel": "update",
    "method": "PATCH"
  },
  {
    "href": "/payments/@payment_id/refund",
    "id": {
      "payment_id": "PAYMENT-5678TYUI"
    },
    "rel": "refund",
    "method": "POST"
  }
],
"links": null
}
```

Response Example (400 Bad Request)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "400",
    "returnReason": "<Corresponding Error Message>",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responsetime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "request_result": {
      "api_gateway": {
        "code": "999999",
        "message": "System Error"
      },
      "payment_gateway": {
        "code": null,
        "message": "FAILED"
      }
    }
  }
}
```

Payments

You can accept payments from your customers by integrating your website or app with Hosted Payment Page serving different payment methods.

Please see the following checkout solutions:

IMPORTANT NOTE:

Conditions may apply to the availability of each checkout solution and its associated payment options, please check with our support team for details.

Hosted Payment Page

Overview The Hosted Payment Page (HPP) is a PCI DSS v3.2 compliant redirect solution, allowing you capture card data without having to worry about the PCI overhead associated with a traditional API integration.

- **Debit / Credit Cards** - Card Data is captured securely inside HPP
- **Equated Monthly Instalment (EMI)** - An option available during the Credit Card checkout process

Supported Payment Options

- **Internet Banking** - Redirect to Bank's Checkout page
- **Mobile Banking** - Redirect to Bank's App while the checkout process is conducted on mobile device
- **eWallet** - Redirect to eWallet's App while the checkout process is conducted on mobile device

Payment Link

A Payment URL link you can embed directly in your website, an SMS or an email. The link will be returned in response field

PATH: `$.response.payment.payment_method`
`.hosted_payment.access_method.payment_link`

Payments

Create a Payment for an Order

INTRODUCTION
[Description](#)
[Update Log](#)
[How to Read this Document](#)
[Features Overview](#)

GETTING STARTED

[How to Connect](#)
[API Gateway URL](#)
[API Authentication](#)
[User Identification](#)
[Connection Security](#)
[Message Security](#)
[Sign & Encrypt](#)
[Decrypt & Verify](#)
[Summary](#)

[How to make API request](#)
with Plain Message
with Data Encryption

[Data Type Overview](#)

[FAQ](#)

[SSL Connection](#)
[Message Encryption](#)
[JOSE Framework](#)

API OPERATIONS

[Orders](#)
[Create Order](#)
[Retrieve Order by ID](#)

Payments

[Create Payment for an Order](#)
[Retrieve Payment by ID](#)
[Update a Payment](#)

Refunds

[Create Refund for a Payment](#)
[Retrieve Refund by ID](#)

Webhooks

[Payments](#)

API SCHEMA

[Schema Definitions](#)
[OrderInput](#)
[OrderOutput](#)
[Order](#)
[PaymentInput](#)
[PaymentPatch](#)
[PaymentOutput](#)
[PaymentWebhook](#)
[Payment](#)
[RefundInput](#)
[RefundOutput](#)
[Refund](#)
[Item](#)
[Card](#)
[HAL](#)
[Exception](#)
[System](#)
[Callback](#)
[Metadata](#)

REFERENCE

[Lifecycle of Cryptographic Keys](#)
[Key Generation & Exchange](#)
[Key Maintenance](#)
[Key Renewal](#)

DISCLAIMER

[Disclaimer](#)

DESCRIPTION

This endpoint creates a Payment which links to a specific Order.

REQUEST PARAMETERS

Authorization BASIC [Base64-encoded Credential]
required
in header

x-hsbc-profileid [Profile ID]
required
in header

x-hsbc-msg-encrypt-id [Merchant ID]+[JWS ID]+[JWE ID]
required
in header

Content-Type application/json
required
in header

id: string Unique `id` of `order`
required
in path *Data Encryption is enforced.*

REQUEST BODY

PaymentInput *Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.*

RESPONSES

200 OK Successful operation.

PaymentOutput *Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.*

400 Bad Request Missing or invalid Parameters.

Exception

403 Forbidden Authorization credentials are missing or invalid.

404 Not Found Empty resource/resource not found.

500 Internal Server Error The request failed due to an internal error.

Request Content-Types: application/json

Request Example

```
{
  "payment_method": {
    "hosted_payment": {
      "url_settings": {
        "return_page": {
          "success": "https://merchant.com/returnPageSuccess",
          "fail": "https://merchant.com/returnPageFail",
          "cancel": "https://merchant.com/returnPageCancel"
        },
        "notification": "https://merchant.com/returnStatus"
      },
      "card_option": [
        "city_visa",
        "bankasia"
      ],
      "billing": {
        "first_name": "khana",
        "last_name": "riphata",
        "email": "khana.riphata@sekha.com",
        "phone": "+01054 694200",
        "street1": "71 Dit Road, 4th Floor",
        "street2": "Malibagh Chowdhury Para",
        "city": "Dhaka",
        "state": "Dhaka",
        "postal_code": "n/a",
        "country": "Bangladesh"
      }
    }
  }
}
```

Response Content-Types: application/json

Response Example (200 OK)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "resultCode": "200",
    "returnReason": "Successful operation",
    "sentTime": "2016-11-15T0:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "payment": {
      "id": "PAYMENT-5678TYUI",
      "bank_tran_id": null,
      "created_at": "2021-06-11T12:10:25Z",
      "last_modified": null,
      "amount": null,
      "store_amount": null,
      "currency": null,
      "status": "PENDING",
      "payment_method": {
        "hosted_payment": {
          "access_method": {
            "payment_link": "https://pay.sandbox.realexpayments.com/card.html?guid=f82dc878-4752-d425-8c4b-7d48b3a863ec"
          },
          "url_settings": {
            "return_page": {
              "success": "https://merchant.com/returnPageSuccess",
              "fail": "https://merchant.com/returnPageFail",
              "cancel": "https://merchant.com/returnPageCancel"
            },
            "notification": "https://merchant.com/returnStatus"
          },
          "card_option": [
            "city_visa",
            "bankasia"
          ],
          "payment_option": null,
          "billing": {
            "first_name": "khana",
            "last_name": "riphata",
            "email": "khana.riphata@sekha.com",
            "phone": "+01054 694200",
            "street1": "71 Dit Road, 4th Floor",
            "street2": "Malibagh Chowdhury Para",
            "city": "Dhaka",
            "state": "Dhaka",
            "postal_code": "n/a",
            "country": "Bangladesh"
          }
        }
      },
      "metadata": null,
      "links": [
        {
          "href": "/payments/@payment_id",
          "id": {
            "payment_id": "PAYMENT-5678TYUI"
          },
          "rel": "self",
          "method": "GET"
        },
        {
          "href": "/payments/@payment_id",
          "id": {
            "payment_id": "PAYMENT-5678TYUI"
          },
          "rel": "update",
          "method": "PATCH"
        }
      ]
    }
  }
}
```

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

```
        ],
        "links": [
            {
                "href": "/orders/@order_id",
                "id": {
                    "order_id": "ORDER-1234QWER"
                },
                "rel": "order",
                "method": "GET"
            }
        ]
    }
}
```

Response Example (400 Bad Request)

```
{
    "system": {
        "messageId": "89817674-da00-4883",
        "returnCode": "400",
        "returnReason": "<Corresponding Error Message>",
        "sentTime": "2016-11-15T10:00:00.000Z",
        "responsetime": "2016-11-15T10:00:00.000Z"
    },
    "response": {
        "request_result": {
            "api_gateway": {
                "code": "999999",
                "message": "System Error"
            },
            "payment_gateway": {
                "code": null,
                "message": "FAILED"
            }
        }
    }
}
```

Retrieve a particular Payment by ID

Payments

GET /payments/{id}

DESCRIPTION

This endpoint retrieves the details of a particular Payment.

REQUEST PARAMETERS

Authorization: BASIC [Base64-encoded Credential]

required

in header

x-hsbc-profileid: [Profile ID]

required

in header

x-hsbc-msg-encrypt-id: [Merchant ID]+[JWS ID]+[JWE ID]

required

in header

Content-Type: application/json

required

in header

id: string Unique `id` of `payment`

required

in path

Data Encryption is enforced.

RESPONSES

200 OK

PaymentOutput

Successful operation.

*Data Encryption is enforced. API Schema
intends to demonstrate the skeleton of the
message payload only.*

400 Bad Request

Exception

Missing or invalid Parameters.

403 Forbidden

Authorization credentials are missing or
invalid.

404 Not Found

Empty resource/resource not found.

500 Internal Server Error

The request failed due to an internal error.

Response Content-Types: application/json

Response Example (200 OK)

```
{
    "system": {
        "messageId": "89817674-da00-4883",
        "returnCode": "200",
        "returnReason": "Successful operation",
        "sentTime": "2016-11-15T10:00:00.000Z",
        "responsetime": "2016-11-15T10:00:00.000Z"
    },
    "response": {
        "payment": {
            "id": "PAYMENT-5678TUYI",
            "bank_tran_id": "210907151716rJv7gJ1f7FkJ6ZI",
            "created_at": "2021-06-11T14:10:25Z",
            "last_modified": "2021-06-12T14:10:25Z",
            "amount": 1000,
            "store_amount": 975,
            "currency": "BDT",
            "status": "VALID",
            "payment_method": {
                "hosted_payment": {
                    "access_method": {
                        "payment_link": "https://pay.sandbox.realexpayments.com/card.html?guid=f82dc878-4752-4d25-8c4b-7d48b3a863ec"
                    },
                    "url_settings": {
                        "return_page": {
                            "url": "https://www.example.com/payment-success"
                        }
                    }
                }
            }
        }
    }
}
```

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

```
"success":  
  "https://merchant.com/returnPageSuccess",  
  "fail": "https://merchant.com/returnPageFail",  
  "cancel":  
    "https://merchant.com/returnPageCancel"  
  },  
  "notification":  
    "https://merchant.com/returnStatus"  
  },  
  "card_option": [  
    "city_visa",  
    "bankasia"  
  ],  
  "payment_option": "CARD",  
  "billing": {  
    "first_name": "khana",  
    "last_name": "riphata",  
    "email": "khana.riphata@sekha.com",  
    "phone": "01054 694200",  
    "street1": "71 Dit Road, 4th Floor",  
    "street2": "Malibagh Chowdhury Para",  
    "city": "Dhaka",  
    "state": "Dhaka",  
    "postal_code": "n/a",  
    "country": "Bangladesh"  
  },  
  "card": {  
    "brand": "VISA-City Bank",  
    "issuer": "TRUST BANK, LTD.",  
    "mcn": "418117XXXXXX6675"  
  }  
},  
"metadata": null,  
"links": [  
  {  
    "href": "/refunds/@refund_id",  
    "id": {  
      "refund_id": "5a61934a4a531"  
    },  
    "rel": "refund",  
    "method": "GET"  
  },  
  {  
    "href": "/refunds/@refund_id",  
    "id": {  
      "refund_id": "8vc78653wn453"  
    },  
    "rel": "refund",  
    "method": "GET"  
  },  
  {  
    "href": "/payments@payment_id/refund",  
    "id": {  
      "payment_id": "PAYMENT-5678TYUI"  
    },  
    "rel": "refund",  
    "method": "POST"  
  },  
  {  
    "href": "/payments@payment_id",  
    "id": {  
      "payment_id": "PAYMENT-5678TYUI"  
    },  
    "rel": "update",  
    "method": "PATCH"  
  }  
],  
"links": [  
  {  
    "href": "/orders/@order_id",  
    "id": {  
      "order_id": "ORDER-1234QWER"  
    },  
    "rel": "order",  
    "method": "GET"  
  }  
]  
}
```

Response Example (400 Bad Request)

```
{  
  "system": {  
    "messageId": "89917674-da00-4883",  
    "returnCode": "400",  
    "returnReason": "<Corresponding Error Message>",  
    "sentTime": "2016-11-15T10:00:00.000Z",  
    "responseTime": "2016-11-15T10:00:00.000Z"  
  },  
  "response": {  
    "request_result": {  
      "api_gateway": {  
        "code": "999999",  
        "message": "System Error"  
      },  
      "payment_gateway": {  
        "code": null,  
        "message": "FAILED"  
      }  
    }  
  }  
}
```

Payments

Update a Payment

PATCH /payments/{id}

DESCRIPTION

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview

FAQ

SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

```
        "method": "PATCH"
      },
      {
        "href": "/refunds/@refund_id",
        "id": {
          "refund_id": "5a61934a4a531"
        },
        "rel": "refund",
        "method": "GET"
      },
      {
        "href": "/refunds/@refund_id",
        "id": {
          "refund_id": "8vc78653wn453"
        },
        "rel": "refund",
        "method": "GET"
      },
      {
        "href": "/payments/@payment_id/refund",
        "id": {
          "payment_id": "PAYMENT-5678TYUI"
        },
        "rel": "refund",
        "method": "POST"
      }
    ],
    "links": [
      {
        "href": "/orders/@order_id",
        "id": {
          "order_id": "ORDER-1234QWER"
        },
        "rel": "order",
        "method": "GET"
      }
    ]
  }
}
```

Response Example (400 Bad Request)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "400",
    "returnReason": "<Corresponding Error Message>",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "request_result": {
      "api_gateway": {
        "code": "999999",
        "message": "System Error"
      },
      "payment_gateway": {
        "code": null,
        "message": "FAILED"
      }
    }
  }
}
```

Refunds

You can make full or partial refunds to customers. Only a settled payment can be refunded.

Refunds

Create a Refund for a Payment

POST /payments/{id}/refund

DESCRIPTION

This endpoint creates a Refund which links to a specific Payment.

REQUEST PARAMETERS

Authorization BASIC [Base64-encoded Credential]

required
in header

x-hsbc-profileid [Profile ID]

required
in header

x-hsbc-msg-encrypt-id [Merchant ID]+[JWS ID]+[JWE ID]

required
in header

Content-Type application/json

required
in header

id: string Unique id of payment

required
in path

Data Encryption is enforced.

Request Content-Types: application/json

Request Example

```
{
  "amount": 1000,
  "currency": "BDT"
}
```

REQUEST BODY

RefundInput *Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.*

RESPONSES

200 OK Successful operation.

RefundOutput *Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.*

400 Bad Request Exception Missing or invalid Parameters.

403 Forbidden Authorization credentials are missing or invalid.

404 Not Found Empty resource/resource not found.

500 Internal Server Error The request failed due to an internal error.

Response Content-Types: application/json

Response Example (200 OK)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "200",
    "returnReason": "Successful operation",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "refund": {
      "id": "6141affc4a2ea",
      "refund_ref_id": "6141affc4a2ea",
      "created_at": "2021-06-11T14:10:25Z",
      "last_modified": null,
      "amount": 1000,
      "currency": "BDT",
      "status": "success",
      "metadata": {
        "refund_reason": "Product is damaged"
      },
      "links": [
        {
          "href": "/refunds/@refund_id",
          "id": {
            "refund_id": "6141affc4a2ea"
          },
          "rel": "self",
          "method": "GET"
        }
      ],
      "links": [
        {
          "href": "/payment/@payment_id",
          "id": {
            "order_id": "PAYMENT-5678TYUI"
          },
          "rel": "payment",
          "method": "GET"
        }
      ]
    }
  }
}
```

Response Example (400 Bad Request)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "400",
    "returnReason": "<Corresponding Error Message>",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "request_result": {
      "api_gateway": {
        "code": "999999",
        "message": "System Error"
      },
      "payment_gateway": {
        "code": null,
        "message": "FAILED"
      }
    }
  }
}
```

Retrieve a particular Refund by ID

Refunds

GET /refunds/{id}

DESCRIPTION

This endpoint retrieves the details of a particular Refund.

REQUEST PARAMETERS

Authorization BASIC [Base64-encoded Credential]
required
in header

x-hsbc-profileid [Profile ID]
required
in header

x-hsbc-msg-encrypt-id [Merchant ID]+[JWS ID]+[JWE ID]
required
in header

Content-Type application/json
required

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview

FAQ

SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments

Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds

Create Refund for a Payment
Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

id: string Unique `id` of `refund`
required in path

Data Encryption is enforced.

RESPONSES

200 OK

RefundOutput

Successful operation.

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

400 Bad Request

Exception

Missing or invalid Parameters.

403 Forbidden

Authorization credentials are missing or invalid.

404 Not Found

Empty resource/resource not found.

500 Internal Server Error

The request failed due to an internal error.

Response Content-Types: application/json

Response Example (200 OK)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "200",
    "returnReason": "Successful operation",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "refund": {
      "id": "6141affc4a2ea",
      "refund_ref_id": "6141affc4a2ea",
      "created_at": "2021-06-11T14:10:25Z",
      "last_modified": null,
      "amount": 1000,
      "currency": "BDT",
      "status": "refunded",
      "metadata": {
        "refund_reason": "Product is damaged"
      },
      "links": null
    },
    "links": [
      {
        "href": "/payment/@payment_id",
        "id": {
          "order_id": "PAYMENT-5678TYUI"
        },
        "rel": "payment",
        "method": "GET"
      }
    ]
  }
}
```

Response Example (400 Bad Request)

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "400",
    "returnReason": "<Corresponding Error Message>",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "request_result": {
      "api_gateway": {
        "code": "999999",
        "message": "System Error"
      },
      "payment_gateway": {
        "code": null,
        "message": "FAILED"
      }
    }
  }
}
```

Webhooks

What is a Webhook

Webhooks (Web Callback, HTTP Push API or Reverse API) is one way one web application can send information to another application in real-time when a specific event happens.

You can use HSBC Omni Collect Webhooks to receive notifications when a specific event occurs. When one of these events is triggered, we send an HTTP POST payload in encrypted JSON to the webhook's configured URL.

Set Up

| Entity | Event | URL Set Up |
|----------|--|---|
| Payments | <ul style="list-style-type: none"> payment.captured payment.failed | Define in <code>\$.payment_method.hosted_payment.url_settings.notification</code> when creating a <code>payment</code> resource |

Exception Handling

Every event that receives a non-2xx response is considered as an event delivery failure and retry mechanism will be triggered. Up to 4 retries will be triggered in every 2 minutes. Maximum 5 calls including the 1st attempt.

Idempotency

There could be scenarios where your endpoint might receive the same webhook multiple times. This could happen as an expected behaviour such as the retry mechanism or any other exceptional behaviour such as network problem.

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

Webhooks

Webhooks for Payments

POST /<Callback URL predefined by Merchant>

DESCRIPTION

The table below lists the Webhook events available for payments.

| Webhook Event | Definition |
|------------------|--|
| payment.captured | Triggered when a payment is successfully captured. |
| payment.failed | Triggered when a payment fails. |

REQUEST PARAMETERS

x-hsbc-webhook-id UUID

required
in header

Content-Type: string text/plain

required
in header

REQUEST BODY

PaymentWebhook

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

Request Content-Types: text/plain

Request Example

```
{
  "webhook": {
    "event": "payment.captured",
    "entities": [
      "payment"
    ],
    "payload": {
      "payment": {
        "id": "PAYMENT-5678TYUI",
        "bank_tran_id": "PAYMENT-5678TYUI",
        "created_at": "2021-06-11T14:10:25Z",
        "last_modified": null,
        "amount": 1000,
        "store_amount": 975,
        "currency": "BDT",
        "status": "VALID",
        "payment_method": {
          "hosted_payment": {
            "access_method": {
              "payment_link": "https://pay.sandbox.realexpayments.com/card.html?guid=f82dc878-4752-4d25-8c4b-7d48b3a863ec"
            },
            "url_settings": {
              "return_page": {
                "success": "https://merchant.com/returnPageSuccess",
                "fail": "https://merchant.com/returnPageFail",
                "cancel": "https://merchant.com/returnPageCancel"
              },
              "notification": "https://merchant.com/returnStatus"
            }
          },
          "card_option": [
            "city_visa",
            "bankasia"
          ],
          "payment_option": "CARD",
          "billing": {
            "first_name": "khana",
            "last_name": "riphata",
            "email": "khana.riphata@sekha.com",
            "phone": "01054 694200",
            "street1": "71 Dit Road, 4th Floor",
            "street2": "Malibagh Chowdhury Para",
            "city": "Dhaka",
            "state": "Dhaka",
            "postal_code": "n/a",
            "country": "Bangladesh"
          },
          "card": {
            "brand": "VISA-City Bank",
            "issuer": "TRUST BANK, LTD.",
            "mcn": "418117XXXXXX6675"
          },
          "emi": {
            "description": "3 Months - 3.50 % FlexiBuy Commission",
            "instalment": 3,
            "issuer": "CITY BANK LIMITED"
          }
        },
        "metadata": {
          "customer_id": "12345",
          "customer_comment": "engrave customer's name on product"
        },
        "links": null
      }
    }
  }
}
```

RESPONSES

200 OK Successful operation.

Callback

Data Encryption is enforced. API Schema intends to demonstrate the skeleton of the message payload only.

Response Content-Types: application/json

Response Example (200 OK)

```
{
  "status": "SUCCESS"
}
```

Schema Definitions

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED
How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption
Data Type Overview
FAQ
SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS
Orders
Create Order
Retrieve Order by ID
Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment
Refunds
Create Refund for a Payment
Retrieve Refund by ID
Webhooks
Payments

API SCHEMA
Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE
Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER
Disclaimer

OrderInput: object

PROPERTIES

txn_reference: string range: (up to 30 chars) required

Unique Transaction Reference defined by Merchant, it will be appeared to be the unique `id` of an `order`.

amount: integer range: $1 \leq x \leq 999999999999$ required

Order Amount

- Format: Eliminate punctuation and sign, support 2 decimal places according to ISO 4217, e.g. 10.50 = 1050

currency: string enum: [BDT] range: (up to 3 chars) required

Order Currency

items: Array<`Item`> range: (up to 20 objects) required

List of Product Descriptions in the basket

metadata: Metadata range: (up to 20 objects) optional

Key-value pair that can be used to store additional information about the entity.

payment: PaymentInput conditional

Required when query parameter `$expand=payment` is opted in. Including this will create `order` and `payment` resources in one-go.

Example

```
{  
  "txn_reference": "ORDER-1234QWER",  
  "amount": 1000,  
  "currency": "BDT",  
  "items": [  
    {  
      "product_name": "Product Item 1",  
      "product_id": "prod-9ijn8uhb",  
      "unitAmt": 900,  
      "unit": 1,  
      "vat": 100,  
      "subAmt": 1000  
    }  
,  
    {"metadata": null,  
     "payment": {  
       ...Refer to schema PaymentInput for details...  
     }  
  }  
}
```

OrderOutput: object

PROPERTIES

system: System required

response: object optional

Return if it is a HTTP 200 response

PROPERTIES

order: Order required

Example

```
{  
  "system": {  
    ...Refer to schema System for details...  
  },  
  "response": {  
    "order": {  
      ...Refer to schema Order for details...  
    }  
  }  
}
```

Order: object

PROPERTIES

id: string range: (up to 50 chars) required

Unique Entity ID of an Order, technically derived from `txn_reference`

txn_reference: string range: (up to 50 chars) required

Unique Transaction Reference defined by Merchant, it will be appeared to be the unique `id` of an `order`.

created_at: string range: (up to 25 chars) required

Creation time of the Order

- Format: `yyyy-MM-dd'T'HH:mm:ss±hh:mm`

Bangladesh Local time

last_modified: string range: (up to 25 chars) required

Last modified time of the Order

- Format: `yyyy-MM-dd'T'HH:mm:ss±hh:mm`

Bangladesh Local time

amount: integer range: $1 \leq x \leq 999999999999$ required

Order Amount

- Format: Eliminate punctuation and sign, support 2 decimal places according to ISO 4217, e.g. 10.50 = 1050

currency: string enum: [BDT] range: (up to 3 chars) required

Order Currency

items: Array<`Item`> required

List of Product Descriptions in the basket

metadata: Metadata range: (up to 20 objects) optional

Key-value pair that can be used to store additional information about the entity.

payments: Array<`Payment`> conditional

List of all payments linked with this Order, appear if query parameter `$expand=payment` is opted in.

links: Array<`HAL`> conditional

Example

```
{  
  "id": "ORDER-1234QWER",  
  "txn_reference": "ORDER-1234QWER",  
  "created_at": "2021-06-11T12:10:25+06:00",  
  "last_modified": "2021-06-12T15:00:25+06:00",  
  "amount": 1000,  
  "currency": "BDT",  
  "items": [  
    {  
      "product_name": "Product Item 1",  
      "product_id": "prod-9ijn8uhb",  
      "unitAmt": 900,  
      "unit": 1,  
      "vat": 100,  
      "subAmt": 1000  
    }  
,  
    {"metadata": null,  
     "payments": [  
       {  
         ...Refer to schema Payment for details...  
       }  
     ],  
     "links": [  
       {  
         "href": "/orders/@order_id",  
         "id": {  
           "order_id": "ORDER-1234QWER"  
         },  
         "rel": "self",  
         "method": "GET"  
       },  
       {  
         "href": "/orders/@order_id/payment",  
         "id": {  
           "order_id": "ORDER-1234QWER"  
         },  
         "rel": "payment",  
         "method": "POST"  
       },  
       {  
         "href": "/payments/@payment_id",  
         "id": {  
           "payment_id": "PAYMENT-5678TYUI"  
         },  
         "rel": "payment",  
         "method": "GET"  
       }  
     ]  
   }  
}
```

PaymentInput: object

PROPERTIES

payment_method: object required

`hosted_payment` is the only choice at this moment.

PROPERTIES

hosted_payment: object conditional

Invoke this object if the payment is processed by Hosted Payment.

PROPERTIES

url_settings: object required

URL setting for Hosted Payment Page

PROPERTIES

return_page: required

URL defined by Merchant for redirecting back to Merchant's website after the payment process is completed in the HPP.

PROPERTIES

success: string range: (up to 255 chars) required

Define for a successful payment

fail: string range: (up to 255 chars) required

Define for a failed payment

cancel: string range: (up to 255 chars) required

Define for a cancelled payment

notification: string range: (up to 255 chars) required

URL defined by Merchant for receiving [Payment Webhooks](#).

card_option: string[] optional

Opt in Card Option(s) to be displayed in the HPP, can be multiple. If no value is provided, all possible options will be displayed.

| Possible Value | Definition |
|-------------------|----------------------------|
| brac_visa | BRAC VISA |
| dbbl_visa | Dutch Bangla VISA |
| city_visa | City Bank Visa |
| ebl_visa | EBL Visa |
| sbl_visa | Southeast Bank Visa |
| brac_master | BRAC MASTER |
| dbbl_master | MASTER Dutch-Bangla |
| city_master | City Master Card |
| ebl_master | EBL Master Card |
| sbl_master | Southeast Bank Master Card |
| city_amex | City Bank AMEX |
| qcash | QCash |
| dbbl_nexus | DBBL Nexus |
| bankasia | Bank Asia IB |
| abbank | AB Bank IB |
| ibbl | IBBL IB and Mobile Banking |
| mtbl | Mutual Trust Bank IB |
| bkash | Bkash Mobile Banking |
| dbblmobilebanking | DBBL Mobile Banking |
| city | City Touch IB |

ITEMS

string enum: [brac_visa, dbbl_visa, city_visa, ebl_visa, sbl_visa, brac_master, dbbl_master, city_master, ebl_master, sbl_master, city_amex, qcash, dbbl_nexus, bankasia, abbank, ibbl, mtbl, bkash, dbblmobilebanking, city]

billing: object required

PROPERTIES

first_name: string range: (up to 25 chars) required

Example

```
{  
  "payment_method": {  
    "hosted_payment": {  
      "url_settings": {  
        "return_page": {  
          "success": "<code>https://merchant.com/returnPageSuccess</code>",  
          "fail": "<code>https://merchant.com/returnPageFail</code>",  
          "cancel": "<code>https://merchant.com/returnPageCancel</code>",  
          "notification": "<code>https://merchant.com/returnStatus</code>"  
        },  
        "card_option": [  
          "city_visa",  
          "bankasia"  
        ],  
        "billing": {  
          "first_name": "khana",  
          "last_name": "riphata",  
          "email": "khana.riphata@sekha.com",  
          "phone": "+8801654 694200",  
          "street1": "71 Dit Road, 4th Floor",  
          "street2": "Malibagh Chowdhury Para",  
          "city": "Dhaka",  
          "state": "Dhaka",  
          "postal_code": "n/a",  
          "country": "Bangladesh"  
        }  
      }  
    }  
  }  
}
```

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview

FAQ

SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER
Disclaimer

Customer's first name. The value should be the same as the value that appears on the card.

last_name: string range: (up to 25 chars) required

Customer's last name. The value should be the same as the value that appears on the card.

email: string range: (up to 50 chars) required

Customer's email address

phone: string range: (up to 20 chars) optional

Customer's Phone Number

street1: string range: (up to 50 chars) optional

First line of the customer's billing address.

street2: string range: (up to 50 chars) optional

Second line of the customer's billing address.

city: string range: (up to 50 chars) optional

The city of the customer's billing address.

state: string range: (up to 50 chars) optional

The city of the customer's billing address.

postal_code: string range: (up to 30 chars) optional

ZIP or other postal code customer's billing address.

country: string range: (up to 50 chars) optional

The country of the customer's billing address.

PaymentPatch: object

PROPERTIES

metadata: Metadata range: (up to 20 objects) optional

Key-value pair that can be used to store additional information about the entity.



NOTE:

Updating metadata in here will replace existing record.

Example

```
{  
  "metadata": {  
    "customer_id": "12345",  
    "customer_comment": "engrave customer's name on product"  
  }  
}
```

PaymentOutput: object

PROPERTIES

system: System required

response: object optional

Return if it is a HTTP 200 response

PROPERTIES

payment: Payment required

links: Array< HAL > required

List of all related resources.



NOTE:

The HAL object in here indicates the immediate parent entity or entities of the entity [payment].

Example

```
{  
  "system": {  
    ...Refer to schema System for details...  
  },  
  "response": {  
    "payment": {  
      ...Refer to schema Payment for details...  
    },  
    "links": [  
      {  
        "href": "/orders/@order_id",  
        "id": {  
          "order_id": "ORDER-1234QWER"  
        },  
        "rel": "order",  
        "method": "GET"  
      }  
    ]  
  }  
}
```

PaymentWebhook: object

PROPERTIES

webhook: object required

PROPERTIES

event: string enum: [payment.captured, payment.failed] range: (up to 100 chars) required

Event Type

entities: string[] required

The list of Entities contained in this Webhook

ITEMS

string enum: [payment]

payload: object required

PROPERTIES

Example

```
{  
  "webhook": {  
    "event": "payment.captured",  
    "entities": [  
      "payment"  
    ],  
    "payload": {  
      "payment": {  
        ...Refer to schema Payment for details...  
      }  
    }  
  }  
}
```

GETTING STARTED

Data Type Overview

API OPERATIONS

API SCHEMA

REFERENCE

DISCLAIMER

Payment: object

PROPERTIES

id: string range: (up to 50 chars) **required**

Unique Entity ID of a Payment

bank_tran_id: string range: (up to 50 chars) **required**

Bank Transaction Reference ID. A unique reference generated by Payment Gateway

created_at: string range: (up to 25 chars) **required**

Creation Time of the payment

- Format: `yyyy-MM-dd'T'HH:mm:ss±hh:mm`

Bangladesh Local time

last_modified: string range: (up to 25 chars) **required**

Last Modified Time of the payment

- Format: `yyyy-MM-dd'T'HH:mm:ss±hh:mm`

Bangladesh Local time

amount: integer range: $1 \leq x \leq 999999999999$ **required**

Payment Amount

- Format: Eliminate punctuation and sign, support 2 decimal places according to ISO 4217, e.g. `10.50 = 1050

store_amount: integer range: $1 \leq x \leq 999999999999$ **required**

The amount what you will get in your account after bank charge (Example: 100 BDT will be your store amount of 96 BDT after 4% Bank Commission)

- Format: Eliminate punctuation and sign, support 2 decimal places according to ISO 4217, e.g. `10.50 = 1050

currency: string enum: [BDT] range: (up to 3 chars) **required**

Payment Currency

status: string enum: [VALID, VALIDATED, PENDING, FAILED] range: (up to 20 chars) **required**

Payment Status

| Possible Value | Definition |
|----------------|---|
| VALID | A successful transaction. |
| VALIDATED | A successful transaction but called by your end more than one. |
| PENDING | The transaction is still not completed and waiting to get the status. |
| FAILED | The transaction is failed. |

payment_method: object **required**

`hosted_payment` is the only choice at this moment.

PROPERTIES

hosted_payment: object **conditional**

Return if the payment is processed by Hosted Payment.

PROPERTIES

access_method: object **required**

The available method(s) of accessing the Payment Page

PROPERTIES

payment_link: string range: (up to 1024 chars) **required**

A Payment URL link a merchant can embed directly in a website, an SMS or an email.

url_settings: object **required**

URL settings for the Hosted Payment Page

PROPERTIES

return_page: object **required**

URL defined by Merchant for redirecting back to Merchant's website after the payment process is completed in the HPP.

PROPERTIES

success: string range: (up to 255 chars) **required**

Define for a successful payment

fail: string range: (up to 255 chars) **required**

Define for a failed payment

cancel: string range: (up to 255 chars) **required**

Define for a cancelled payment

notification: string range: (up to 255 chars) **required**

URL defined by Merchant for receiving [Payment Webhooks](#).

Example

```
{
  "id": "PAYMENT-5678TYUI",
  "bank_tran_id": "PAYMENT-5678TYUI",
  "created_at": "2021-06-11T14:10:25Z",
  "last_modified": "2021-06-12T14:10:25Z",
  "amount": 1000,
  "store_amount": 975,
  "currency": "BDT",
  "status": "VALID",
  "payment_method": {
    "hosted_payment": {
      "access_method": {
        "payment_link": "https://pay.sandbox.realexpayments.com/card.html?guid=f82dc878-4752-4d25-8c4b-7d48b3a863ec"
      }
    },
    "url_settings": {
      "return_page": {
        "success": "https://merchant.com/returnPageSuccess",
        "fail": "https://merchant.com/returnPageFail",
        "cancel": "https://merchant.com/returnPageCancel"
      },
      "notification": "https://merchant.com/returnStatus"
    },
    "card_option": [
      "city_visa",
      "bankasia"
    ],
    "payment_option": "CARD",
    "billing": {
      "first_name": "khana",
      "last_name": "riphata",
      "email": "khana.riphata@sekha.com",
      "phone": "+01054_694200",
      "street1": "71 Dit Road, 4th Floor",
      "street2": "Malibagh Chowdhury Para",
      "city": "Dhaka",
      "state": "Dhaka",
      "postal_code": "n/a",
      "country": "Bangladesh"
    },
    "card": {
      "brand": "VISA-City Bank",
      "issuer": "TRUST BANK, LTD.",
      "mcn": "418117XXXXXX6675"
    },
    "emi": {
      "description": "3 Months - 3.50 % FlexiBuy Commission",
      "instalment": 3,
      "issuer": "CITY BANK LIMITED"
    },
    "internet_banking": {
      "issuer": "Bank Asia Limited"
    },
    "mobile_banking": {
      "issuer": "BKash Mobile Banking"
    },
    "ewallet": {
      "issuer": "xxxxxx"
    }
  },
  "metadata": null,
  "refunds": [
    {
      ...Refer to schema Refund for details...
    }
  ],
  "links": [
    {
      "href": "/payments/@payment_id",
      "id": {
        "payment_id": "PAYMENT-5678TYUI"
      },
      "rel": "self",
      "method": "GET"
    },
    {
      "href": "/payments/@payment_id",
      "id": {
        "payment_id": "PAYMENT-5678TYUI"
      },
      "rel": "update",
      "method": "PATCH"
    },
    {
      "href": "/refunds/@refund_id",
      "id": {
        "refund_id": "6141affc4a2ea"
      },
      "rel": "refund",
      "method": "GET"
    },
    {
      "href": "/payments/@payment_id/refund",
      "id": {
        "payment_id": "PAYMENT-5678TYUI"
      },
      "rel": "refund",
      "method": "POST"
    }
  ]
}
```

card_option: string[] [optional]

Opt in Card Option(s) to be displayed in the HPP, can be multiple. If no value is provided, all possible options will be displayed.

| Possible Value | Definition |
|-------------------|----------------------------|
| brac_visa | BRAC VISA |
| dbbl_visa | Dutch Bangla VISA |
| city_visa | City Bank Visa |
| ebl_visa | EBL Visa |
| sbl_visa | Southeast Bank Visa |
| brac_master | BRAC MASTER |
| dbbl_master | MASTER Dutch-Bangla |
| city_master | City Master Card |
| ebl_master | EBL Master Card |
| sbl_master | Southeast Bank Master Card |
| city_amex | City Bank AMEX |
| qcash | QCash |
| dbbl_nexus | DBBL Nexus |
| bankasia | Bank Asia IB |
| abbank | AB Bank IB |
| ibbl | IBBL IB and Mobile Banking |
| mtbl | Mutual Trust Bank IB |
| bkash | Bkash Mobile Banking |
| dbblmobilebanking | DBBL Mobile Banking |
| city | City Touch IB |

ITEMS

```
string enum: [ brac_visa, dbbl_visa, city_visa, ebl_visa, sbl_visa,
  brac_master, dbbl_master, city_master, ebl_master, sbl_master, city_amex,
  qcash, dbbl_nexus, bankasia, abbank, ibbl, mtbl, bkash, dbblmobilebanking,
  city ]
```

payment_option: string enum: [CARD, INTERNET_BANKING,
MOBILE_BANKING, EWALLET] range: (up to 20 chars) [required]

The selected Payment Option used inside the HPP

| Possible Value | Definition |
|------------------|------------------|
| CARD | Card Payment |
| INTERNET_BANKING | Internet Banking |
| MOBILE_BANKING | Mobile Banking |
| EWALLET | E-wallet |

billing: object [required]**PROPERTIES****first_name: string range: (up to 25 chars) [required]**

Customer's first name. The value should be the same as the value that appears on the card.

last_name: string range: (up to 25 chars) [required]

Customer's last name. The value should be the same as the value that appears on the card.

email: string range: (up to 50 chars) [required]

Customer's email address

phone: string range: (up to 20 chars) [optional]

Customer's Phone Number

street1: string range: (up to 50 chars) [optional]

First line of the customer's billing address.

street2: string range: (up to 50 chars) [optional]

Second line of the customer's billing address.

city: string range: (up to 50 chars) [optional]

The city of the customer's billing address.

state: string range: (up to 50 chars) [optional]

The city of the customer's billing address.

postal_code: string range: (up to 30 chars) [optional]

ZIP or other postal code customer's billing address.

country: string range: (up to 50 chars) [optional]

The country of the customer's billing address.

card: Card [conditional]

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview

FAQ

SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders

Create Order
Retrieve Order by ID

Payments

Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds

Create Refund for a Payment
Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

Card Details. Appear if `"payment_option" = "CARD"`
emi: object conditional
EMI Details. Appear if `"payment_option" = "CARD"`

PROPERTIES

description: string range: (up to 100 chars) required
EMI description

instalment: integer range: $1 \leq x \leq 99$ required
EMI instalment period

issuer: string range: (up to 100 chars) required
Issuer

internet_banking: object conditional
Internet Banking Details. Appear if `"payment_option" = "INTERNET_BANKING"`

PROPERTIES

issuer: string range: (up to 100 chars) required
Issuer

mobile_banking: object conditional
Mobile Banking Details. Appear if `"payment_option" = "MOBILE_BANKING"`

PROPERTIES

issuer: string range: (up to 100 chars) required
Issuer

ewallet: object conditional
E-Wallet Details. Appear if `"payment_option" = EWALLET"`

PROPERTIES

issuer: string range: (up to 100 chars) required
Issuer

metadata: Metadata range: (up to 20 objects) optional
Key-value pair that can be used to store additional information about the entity.

refunds: Array< Refund > conditional
List of all Refunds linked with this Payment, appear if query parameter `[$expand=refund]` is opted in.

links: Array< HAL > conditional
List of all related resources. If query parameter `[$expand=refund]` is opted out, refunds will be related here in HAL format.

RefundInput: object

PROPERTIES

amount: integer range: $1 \leq x \leq 999999999999$ required
Refund Amount

- Format: Eliminate punctuation and sign, support 2 decimal places according to ISO 4217, e.g. `~10.50 = 1050`

currency: string enum: [BDT] range: (up to 3 chars) required
Refund Currency

Example

```
{  
  "amount": 1000,  
  "currency": "BDT"  
}
```

RefundOutput: object

PROPERTIES

system: System required
response: object optional
Return if it is a HTTP 200 response

PROPERTIES

refund: Refund required
links: Array< HAL > required
List of all related resources.

NOTE:

The HAL object in here indicates the immediate parent entity or entities of the entity `refund`.

Example

```
{  
  "system": {  
    ...Refer to schema System for details...  
  },  
  "response": {  
    "refund": {  
      ...Refer to schema Refund for details...  
    },  
    "links": [  
      {  
        "href": "/payment/@payment_id",  
        "id": {  
          "order_id": "PAYMENT-5678TYUI"  
        },  
        "rel": "payment",  
        "method": "GET"  
      }  
    ]  
  }  
}
```

[Description](#)[Update Log](#)[How to Read this Document](#)[Features Overview](#)**GETTING STARTED**[How to Connect](#)[API Gateway URL](#)[API Authentication](#)[User Identification](#)[Connection Security](#)[Message Security](#)[Sign & Encrypt](#)[Decrypt & Verify](#)[Summary](#)[How to make API request](#)[with Plain Message](#)[with Data Encryption](#)[Data Type Overview](#)**FAQ**[SSL Connection](#)[Message Encryption](#)[JOSE Framework](#)**API OPERATIONS**[Orders](#)[Create Order](#)[Retrieve Order by ID](#)[Payments](#)[Create Payment for an Order](#)[Retrieve Payment by ID](#)[Update a Payment](#)[Refunds](#)[Create Refund for a Payment](#)[Retrieve Refund by ID](#)[Webhooks](#)[Payments](#)**API SCHEMA**[Schema Definitions](#)[OrderInput](#)[OrderOutput](#)[Order](#)[PaymentInput](#)[PaymentPatch](#)[PaymentOutput](#)[PaymentWebhook](#)[Payment](#)[RefundInput](#)[RefundOutput](#)[Refund](#)[Item](#)[Card](#)[HAL](#)[Exception](#)[System](#)[Callback](#)[Metadata](#)**REFERENCE**[Lifecycle of Cryptographic Keys](#)[Key Generation & Exchange](#)[Key Maintenance](#)[Key Renewal](#)**DISCLAIMER**[Disclaimer](#)

Refund: object

PROPERTIES**id:** string range: (up to 50 chars) **required**Unique Entity ID of a Refund, identical to `refund_ref_id`**refund_ref_id:** string range: (up to 50 chars) **required**

Refund Reference. A unique reference generated by Payment Gateway

created_at: string range: (up to 25 chars) **required**

Creation Time of the Refund

- Format: `yyyy-MM-dd'T'HH:mm:ss±hh:mm`
- Bangladesh Local time

last_modified: string range: (up to 25 chars) **required**

Last Modified Time of the Refund

- Format: `yyyy-MM-dd'T'HH:mm:ss±hh:mm`
- Bangladesh Local time

amount: integer range: $1 \leq x \leq 999999999999$ **required**

Refund Amount

- Format: Eliminate punctuation and sign, support 2 decimal places according to ISO 4217, e.g. `₹10.50 = 1050`

currency: string enum: [BDT] range: (up to 3 chars) **required**

Refund Currency

status: string enum: [success, failed, processing, refunded, cancelled] range: (up to 50 chars) **required**

Refund Status

| Possible Value | Definition |
|----------------|--|
| success | Refund request is initiated successfully |
| failed | Refund request is failed to initiate |
| processing | Refund request is under processing |
| refunded | Refund request has been proceeded successfully |
| cancelled | Refund request has been proceeded successfully |

metadata: Metadata range: (up to 20 objects) **optional**

Key-value pair that can be used to store additional information about the entity.

links: Array< HAL > **conditional**

List of all related resources.

Example

```
{
  "id": "6141afffc4a2ea",
  "refund_ref_id": "6141afffc4a2ea",
  "created_at": "2021-06-11T14:10:25Z",
  "last_modified": "2021-06-12T14:10:25Z",
  "amount": 1000,
  "currency": "BDT",
  "status": "refunded",
  "metadata": null,
  "links": [
    {
      "href": "/refunds/@refund_id",
      "id": {
        "refund_id": "6141afffc4a2ea"
      },
      "rel": "self",
      "method": "GET"
    }
  ]
}
```

Item: object

PROPERTIES**product_name:** string range: (up to 200 chars) **required**

Product Item Name / Description

product_id: string range: (up to 50 chars) **required**

Product Number / ID

unitAmt: integer range: $1 \leq x \leq 999999999999$ **required**

Unit Amount of each item

! NOTE: Do not use comma or dot. For example: Input `10000` instead of `100.00`

unit: integer range: $1 \leq x \leq 9999$ **required**

No. of Unit

vat: integer range: $0 \leq x \leq 999999999999$ **required**

Total VAT Tax Amount for all units

! NOTE: Do not use comma or dot. For example: Input `10000` instead of `100.00`

subAmt: integer range: $1 \leq x \leq 999999999999$ **required**

The Sum of one particular item with multiple orders plus VAT

! NOTE: For example, `unitAmt x unit + vat = subAmt` Do not use comma or dot. For example: Input `10000` instead of `100.00`

Example

```
{
  "product_name": "Product Item 1",
  "product_id": "prod-9ijn8uhb",
  "unitAmt": 900,
  "unit": 1,
  "vat": 100,
  "subAmt": 1000
}
```

[Description](#)[Update Log](#)[How to Read this Document](#)[Features Overview](#)**GETTING STARTED**[How to Connect](#)[API Gateway URL](#)[API Authentication](#)[User Identification](#)[Connection Security](#)[Message Security](#)[Sign & Encrypt](#)[Decrypt & Verify](#)[Summary](#)[How to make API request](#)[with Plain Message](#)[with Data Encryption](#)[Data Type Overview](#)[FAQ](#)[SSL Connection](#)[Message Encryption](#)[JOSE Framework](#)**API OPERATIONS**[Orders](#)[Create Order](#)[Retrieve Order by ID](#)[Payments](#)[Create Payment for an Order](#)[Retrieve Payment by ID](#)[Update a Payment](#)[Refunds](#)[Create Refund for a Payment](#)[Retrieve Refund by ID](#)[Webhooks](#)[Payments](#)**API SCHEMA**[Schema Definitions](#)[OrderInput](#)[OrderOutput](#)[Order](#)[PaymentInput](#)[PaymentPatch](#)[PaymentOutput](#)[PaymentWebhook](#)[Payment](#)[RefundInput](#)[RefundOutput](#)[Refund](#)[Item](#)[Card](#)[HAL](#)[Exception](#)[System](#)[Callback](#)[Metadata](#)**REFERENCE**[Lifecycle of Cryptographic Keys](#)[Key Generation & Exchange](#)[Key Maintenance](#)[Key Renewal](#)**DISCLAIMER**[Disclaimer](#)

Card: object

PROPERTIES

brand: string range: (up to 50 chars) required

Indicates the card brand that issued the card

issuer: string range: (up to 100 chars) required

Card Issuer

mcn: string range: (up to 16 chars) required

Masked card number

Example

```
{
  "brand": "VISA-City Bank",
  "issuer": "TRUST BANK, LTD.",
  "mcn": "418117XXXXXX6675"
}
```

HAL: object

DESCRIPTION

Hypertext Application Language (HAL) is an Open API standard convention for defining hypermedia such as links to related resources within JSON or XML code

PROPERTIES

href: string range: (up to 100 chars) required

URL of the related resource

id: object required

PROPERTIES

entity_id: string range: (up to 100 chars)

Entity ID used in the URL

rel: string range: (up to 100 chars) required

Relation of the Resource

method: string enum: [GET, POST, PATCH, DELETE] range: (up to 100 chars)required

HTTP Method

Example

```
{
  "href": "/entity/@entity_id",
  "id": {
    "entity_id": "entity-111222333"
  },
  "rel": "EntityName",
  "method": "GET"
}
```

Exception: object

PROPERTIES

system: System required**response:** object optional

Return if the exception is taken place in any downstream system

PROPERTIES

request_result: object required

PROPERTIES

api_gateway: object required

Result returned by API Gateway

PROPERTIES

code: string range: (up to 50 chars) required

Result code

message: string range: (up to 100 chars) required

Result message

payment_gateway: object required

Result returned by Payment Gateway

Example

```
{
  "system": {
    "messageId": "89817674-da00-4883",
    "returnCode": "400",
    "returnReason": "<Corresponding Error Message>",
    "sentTime": "2016-11-15T10:00:00.000Z",
    "responseTime": "2016-11-15T10:00:00.000Z"
  },
  "response": {
    "request_result": {
      "api_gateway": {
        "code": "999999",
        "message": "System Error"
      },
      "payment_gateway": {
        "code": null,
        "message": "FAILED"
      }
    }
  }
}
```

System: object

PROPERTIES

messageId: string range: (up to 36 chars) required

System generated unique message ID only for HSBC internal reference use

returnCode: string range: (up to 3 chars) required

System Return Code.

Example

```
{
  "messageId": "89817674-da00-4883",
  "returnCode": "200",
  "returnReason": "RETURN_MESSAGE",
  "sentTime": "2016-11-15T10:00:00.000Z",
  "responseTime": "2016-11-15T10:00:00.000Z"
}
```

- This checking is on API Operational level, in other words, it checks upon Authorization, Connectivity and JSON Message Structure.

INTRODUCTION

Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request

with Plain Message
with Data Encryption

Data Type Overview

FAQ
SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

| Possible Value | Definition |
|----------------|---|
| 200 | Successful operation |
| 400 | Bad Request (With detail message in field <code>returnReason</code>) |
| 500 | Internal Error. Notices: Faster Payment System is a multiple-tiers system, system down or unavailable of any single dependent system (or tier) across the entire FPS pipeline can return HTTP Return Code <code>500</code> with different <code>returnReason</code> . Furthermore, if one tier which comes before the API Cloud Foundry is unavailable, such as the API Gateway, there will be even no json message returned. Developer is suggested to catch the native HTTP Return Code before trying to look into the <code>resultCode</code> in json message. |

returnReason: string range: (up to 200 chars) required

Corresponding Text message of `resultCode`

| Corr. Return Code | Return Message Sample | Definition |
|-------------------|--|--|
| 200 | Successful operation | A successful API operation in terms of Authorization, Connectivity and valid JSON Message Structure. Any checking failure on Business Logic level will be still considered a successful API operation yet the Business Logic checking result will be returned in <code>response</code> object. |
| 400 | Profile ID - Merchant ID mapping is not correct/updated! | The binding of Profile ID, Merchant ID and Merchant Public Certificate is incorrect or not up-to-date. |
| 400 | object has missing required properties [field name] | Fail to pass JSON Field Mandatory Check. |
| 400 | instance type [data type] does not match any allowed primitive type | Fail to pass JSON Field Type Check. |
| 400 | string [field value] is too long | Fail to pass JSON Field Max Length Check |
| 400 | instance failed to match at least one required schema among [no. of conditional field] | Fail to pass JSON Conditional Field Check. |
| 500 | java.net.ConnectException: Connection refused: connect | Notices: Message can be varied depended on the corresponding dependent system which returns this message. Yet, all reasons can be concluded into System Unavailable. |

sentTime: string range: (up to 27 chars) required

Time of request received by HSBC system from client, only for HSBC internal reference use

responseTime: string range: (up to 27 chars) required

Time of HSBC system provides response to client, only for HSBC internal reference use

Callback: object

PROPERTIES

status: string range: (up to 30 chars) required

Return Message

Example

```
{
  "status": "SUCCESS"
}
```

Metadata: object

PROPERTIES

A JSON object delimited by `,`, both `key` and `value` support free-typed string up to 512 chars.

Example

```
{
  "metadata": {
    "key_1": "value_1",
    "key_2": "value_2",
    "key_3": "value_3",
    ...More pairs can be defined below...
  }
}
```

Lifecycle of Cryptographic Keys

INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

This section highlights the Lifecycle of cryptographic keys in the following stages:

1. Generate keys pair (Private Key and Public Key Certificate)
2. **Optional:** Export CSR (Certificate Signing Request) and sign using a CA (Certificate Authority)

DID YOU KNOW?

In public key infrastructure (PKI) systems, a certificate signing request is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. It usually contains the public key for which the certificate should be issued.

3. Exchange Certificate with HSBC
4. Certificate and Keys Maintenance
5. Certificate and Keys Renewal Process

The Key Renewal Process Command line tool **Java Keytool™** is used in the demonstration. The tool can generate public key / private key pairs and store them into a Java KeyStore. The Keytool executable is distributed with the **Java SDK (or JRE)™**, so if you have an SDK installed you will also have the Keytool executable. The Merchant is free to choose any other tool to generate and manage keys, such as **OpenSSL™**.

Key Generation and Certificate Exchange with HSBC

1. Create a new keys pair (Private Key and Public Key Certificate) with a new or existing Keystore.

```
keytool -genkey
    -alias merchant_key_pair
    -keyalg RSA
    -keystore merchant_keystore.jks
    -keysize 2048
    -validity 3650
    -storepass <your keystore password>
```

- **-genkey** - command to generate keys pair.
- **-alias** - define the alias name (or unique identifier) of the keys pair stored inside the keystore.
- **-keyalg** - key algorithm, it must be **RSA** regarding to HSBC standard. If **RSA** is taken, the default hashing algorithm will be **SHA-256**.
- **-keystore** - file name of the keystore. If the file already exists in your system location, the key will be created inside your existing keystore, otherwise, a new keystore with the defined name will be created.

DID YOU KNOW?

Keystore is a password-protected repository of keys and certificates. A file with extension **.jks** means it is a Java Keystore which is originally supported and executable with Java™.

There are several keystore formats in the industry like **.PKCS12** | with file extension **.p12** | which is executable with Microsoft Windows™, merchant can always pick the one most fit their application.

- **-keysize** - key size, it must be **2048** regarding to HSBC standard.
- **-validity** - the validity period of the private key and its associated certificate. The unit is **day**, 3650 means 10 years.
- **-storepass** - password of the keystore.

- 1.1. Provide the **Distinguished Name** information after running the command:

```
Information required for CSR generation
-----
What is your first and last name?
[Unknown]: MERCHANT INFO
What is the name of your organizational unit?
[Unknown]: MERCHANT INFO
What is the name of your organization?
[Unknown]: MERCHANT INFO
What is the name of your City or Locality?
[Unknown]: HK
What is the name of your State or Province?
[Unknown]: HK
What is the two-letter country code for this unit?
[Unknown]: HK
Is CN=XXX, OU=XXX, O=XXX, L=HK, ST=HK, C=HK correct? (type "y" or "n")
[no]: yes

Enter key password for <merchant_key_pair>
(RRETURN if same as keystore password):
Re-enter new password:
```

INTRODUCTION
Description
Update Log
How to Read this Document
Features Overview

GETTING STARTED

How to Connect
API Gateway URL
API Authentication
User Identification
Connection Security
Message Security
Sign & Encrypt
Decrypt & Verify
Summary

How to make API request
with Plain Message
with Data Encryption

Data Type Overview
FAQ
SSL Connection
Message Encryption
JOSE Framework

API OPERATIONS

Orders
Create Order
Retrieve Order by ID

Payments
Create Payment for an Order
Retrieve Payment by ID
Update a Payment

Refunds
Create Refund for a Payment
Retrieve Refund by ID

Webhooks
Payments

API SCHEMA

Schema Definitions
OrderInput
OrderOutput
Order
PaymentInput
PaymentPatch
PaymentOutput
PaymentWebhook
Payment
RefundInput
RefundOutput
Refund
Item
Card
HAL
Exception
System
Callback
Metadata

REFERENCE

Lifecycle of Cryptographic Keys
Key Generation & Exchange
Key Maintenance
Key Renewal

DISCLAIMER

Disclaimer

NOTE:

The Private Key password and Keystore password can be identical, however to be more secure, the Merchant should set them differently.

2. **Optional:** Export CSR and get signed with CA. This step can be skipped if the Merchant decides to work with a Self-Signed Certificate.

```
keytool -certreq  
-alias merchant_key_pair  
-keyalg RSA  
-file merchant_csr.csr  
-keystore merchant_keystore.jks
```

- **-certreq** - command to generate and export CSR.
- **-alias** - the name of the associated keys pair.
- **-keyalg** - key algorithm, it must be **RSA** regarding to HSBC standard.
- **-file** - file name of the CSR. This will be generated at the location where the command is run.
- **-keystore** - specify the keystore which you are working on.

2.1. Select and purchase a plan at Certificate Authority and then submit the CSR accordingly. After a signed Certificate is issued by CA, import the Certificate back to the Merchant's keystore.

```
keytool -import  
-alias merchant_signed_cert_0001  
-trustcacerts -file CA_signed_cert.p7b  
-keystore merchant_keystore.jks
```

- **-import** - command to import object into a specific keystore.
- **-alias** - define the alias name (or unique identifier) of the signed Certificate.
- **-trustcacerts -file** - specify the file name of the signed Certificate in Merchant's local file system.

NOTE:
[PKCS#7] is one of the common formats that contains certificates and has a file extension of **.p7b** or **.p7c**. The certificate format may be varied depending on the policy of the issuing CA.

- **-keystore** - specify the keystore which you are working on.

3. Export the Certificate and send it to HSBC for key exchange.

DID YOU KNOW:

A Certificate or Public Key Certificate is an electronic document that contains a public key and additional information that prove the ownership and maintains integrity of the public key. It is essential for the sender to ensure the key is not altered by any chance during delivery.

```
keytool -export  
-alias merchant_key_pair  
-file merchant_cert_0001.cer  
-keystore merchant_keystore.jks
```

- **-export** - command to export object from a specific keystore.
- **-alias** - the name of the associated keys pair.

NOTE:
If the Merchant associates the original keys pair **merchant_key_pair**, the exported Certificate is without CA-signed, and hence, Self-Signed. However, if the Merchant associates the imported Certificate **merchant_signed_cert_0001** mentioned in step #2, the exported Certificate is CA-signed.

- **-file** - specify the file name of the Certificate where the file will be exported to Merchant's local file system.

NOTE:

The default Certificate file encoding is binary. HSBC accepts both binary and base64 encoding. To export a printable base64 encoding file, please attach an extra parameter **-rfc** in the command.
e.g. **-file merchant_cert_0001.crt -rfc**.

- **-keystore** - specify the keystore which you are working on.

4. Import HSBC's Certificate into the merchant's Keystore.

```
keytool -import  
-alias hsbc_cert_0002  
-file hsbc_cert_0002.cer  
-keystore merchant_keystore.jks
```



- **-import** - command to import object into a specific keystore.
- **-alias** - define the alias name of HSBC's Certificate in your keystore.
- **-file** - specify the file name of HSBC's Certificate in Merchant's local file system.
- **-keystore** - specify the keystore which you are working on.

5. **Optional:** List keystore objects. Merchant is suggested to verify that all required objects are properly maintained. 2 - 3 entries should be found in your Java Keystore: (*Entries may be varied if other key repository format is used*)

| Alias name | Corresponding Object | Remark |
|---------------------------|---|---|
| merchant_key_pair | <ul style="list-style-type: none"> • Merchant's Private Key • Merchant's Public Certificate (Self-Signed) | These two objects appear to be one entry in a JAVA Keystore. Merchant can still export them separately into two objects (files) on your local file system depending on your application design. |
| merchant_signed_cert_0001 | <ul style="list-style-type: none"> • Merchant's Public Certificate (CA-Signed) | Not exist Merchant skips step #2 |
| hsbc_cert_0002 | <ul style="list-style-type: none"> • HSBC's Public Certificate | |

```
keytool -list -v -keystore merchant_keystore.jks

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: merchant_key_pair
Creation date: Jan 1, 2020
Entry type: PrivateKeyEntry

<Other Information>
*****
***** Alias name: merchant_signed_cert_0001
***** Creation date: Jan 1, 2020
***** Entry type: trustedCertEntry

<Other Information>
*****
***** Alias name: hsbc_cert_0002
***** Creation date: Jan 1, 2020
***** Entry type: trustedCertEntry

<Other Information>
*****
```

INTRODUCTION
[Description](#)
[Update Log](#)
[How to Read this Document](#)
[Features Overview](#)

GETTING STARTED
[How to Connect](#)
[API Gateway URL](#)
[API Authentication](#)
[User Identification](#)
[Connection Security](#)
[Message Security](#)
[Sign & Encrypt](#)
[Decrypt & Verify](#)
[Summary](#)

[How to make API request with Plain Message](#)
[with Data Encryption](#)

[Data Type Overview](#)
[FAQ](#)
[SSL Connection](#)
[Message Encryption](#)
[JOSE Framework](#)

API OPERATIONS
[Orders](#)
[Create Order](#)
[Retrieve Order by ID](#)

[Payments](#)
[Create Payment for an Order](#)
[Retrieve Payment by ID](#)
[Update a Payment](#)

[Refunds](#)
[Create Refund for a Payment](#)
[Retrieve Refund by ID](#)

[Webhooks](#)
[Payments](#)

API SCHEMA

[Schema Definitions](#)
[OrderInput](#)
[OrderOutput](#)
[Order](#)
[PaymentInput](#)
[PaymentPatch](#)
[PaymentOutput](#)
[PaymentWebhook](#)
[Payment](#)
[RefundInput](#)
[RefundOutput](#)
[Refund](#)
[Item](#)
[Card](#)
[HAL](#)
[Exception](#)
[System](#)
[Callback](#)
[Metadata](#)

REFERENCE

[Lifecycle of Cryptographic Keys](#)
[Key Generation & Exchange](#)
[Key Maintenance](#)
[Key Renewal](#)

DISCLAIMER

[Disclaimer](#)

Certificates and Keys Maintenance

Here are some recommendations to Merchant of how to properly maintain certificates and keys:

| Component | Storage | Validity |
|-----------|---------|----------|
|-----------|---------|----------|

| | Component | Storage | Validity |
|-----------------------------------|-----------|---|--|
| INTRODUCTION | | Private Key should be maintained and handled with the most secure approach that a Merchant can apply. The most common and yet secure enough approach is: | No restriction on the Validity Period. However, if Merchant suspects there is any chance that the key is leaked or for any other security reason, a new Private Key and its associated Public Key Certificate should be generated. |
| Merchant's Private Key | | <ul style="list-style-type: none"> • key password - Do not save the password in plain text or hard-coded in application. Recommend to encrypt it by any Password Encryption Tools • key storage - Store inside password-protected key repository, such as JKS or PKCS12 keystore. Keystore password should also be encrypted. | |
| Merchant's Public Key Certificate | | <p>Since Public Key Certificate is publicly distributed, a comparative moderate secure storage approach is acceptable. Merchant can store the physical file in any system's file system or store all keys and certificates in one single key repository for a centralised key management.</p> | <p>For a self-signed Certificate, the same condition has been mentioned as above.</p> <p>However, the validity period of a CA-signed Certificate is depended on the purchase plan of the issuing CA. The most common standard is 1 to 2 years.</p> |
| | | | 1 Year |
| HSBC's Public Key Certificate | | Same as the above | <p>NOTE: Technically, the validity period is usually 1 Year plus 1 to 2 months more. The spare period is a buffer for a merchant to switch a "to-be-expired" Certificate to the new one during the Certificate Renewal Process. More technical detail will be covered in later section.</p> |

Certificates and Keys Renewal

Every Public Key Certificate has an expiration date. When either the Merchant's or HSBC's Certificate is about to expire, a key renewal process takes place. Please see the Key Renewal Process Flow below:

- SOME RULES YOU SHOULD KNOW:**
- **Keys Repository:** This is a mock-up for demonstration purpose only.
 - **Keys Name:** Using a **Key Name** **KeyID** naming convention makes for a simpler demonstration. The suggested identifier of one key should be the alias name inside a key repository.
 - **KeyID Value:** HSBC uses the naming convention **0001**, **0002**, **0003** ... **n + 1**, each time the HSBC certificate is renewed, the **KeyID** value is **n + 1**.
 - **KeyID Binding:** The binding between the **KeyID** and the corresponding **Keys Pair** in the merchant's system can make use of any key/value logic, such as a Database table. In our example below, **KeyID 000X** binds to **Private Key v.000X** and **Public Certificate v.000X**, etc.
 - **Validity Date:** All dates are made-up for demonstration purposes only.

INTRODUCTION
 Description
 Update Log
 How to Read this Document
 Features Overview

GETTING STARTED
 How to Connect
 API Gateway URL
 API Authentication
 User Identification
 Connection Security
 Message Security
 Sign & Encrypt
 Decrypt & Verify
 Summary

How to make API request
 with Plain Message
 with Data Encryption
 Data Type Overview
 FAQ
 SSL Connection
 Message Encryption
 JOSE Framework

API OPERATIONS
 Orders
 Create Order
 Retrieve Order by ID
 Payments
 Create Payment for an Order
 Retrieve Payment by ID
 Update a Payment

Refunds
 Create Refund for a Payment
 Retrieve Refund by ID

Webhooks
 Payments

API SCHEMA
 Schema Definitions
 OrderInput
 OrderOutput
 Order
 PaymentInput
 PaymentPatch
 PaymentOutput
 PaymentWebhook
 Payment
 RefundInput
 RefundOutput
 Refund
 Item
 Card
 HAL
 Exception
 System
 Callback
 Metadata

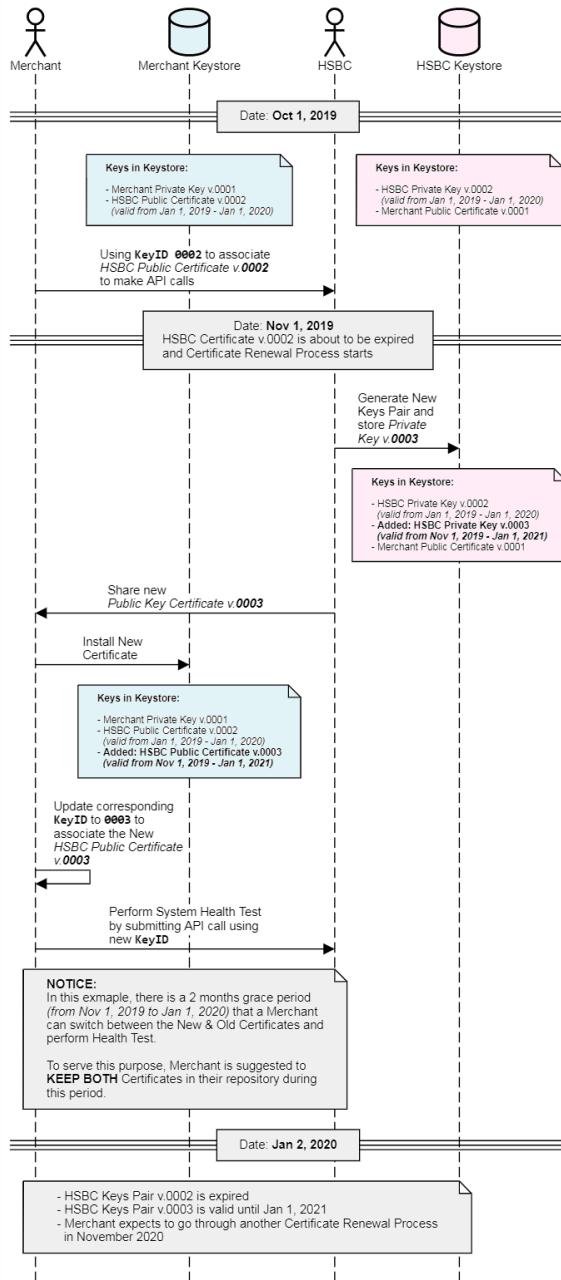
REFERENCE

Lifecycle of Cryptographic Keys
 Key Generation & Exchange
 Key Maintenance
 Key Renewal

DISCLAIMER

Disclaimer

HSBC Public Key Certificate Renewal (Logical Flow)



Below is the technical flow showing how **Certificates**, **Alias Names** and **Key IDs** work together during a normal process or a key renewal process:

INTRODUCTION

- Description
- Update Log
- How to Read this Document
- Features Overview

GETTING STARTED

- How to Connect
- API Gateway URL
- API Authentication
- User Identification
- Connection Security
- Message Security
 - Sign & Encrypt
 - Decrypt & Verify
 - Summary

- How to make API request
- with Plain Message
- with Data Encryption

Data Type Overview

FAQ

- SSL Connection
- Message Encryption
- JOSE Framework

API OPERATIONS

- Orders
 - Create Order
 - Retrieve Order by ID

- Payments
 - Create Payment for an Order
 - Retrieve Payment by ID
 - Update a Payment

Refunds

- Create Refund for a Payment
- Retrieve Refund by ID

Webhooks

- Payments

API SCHEMA

Schema Definitions

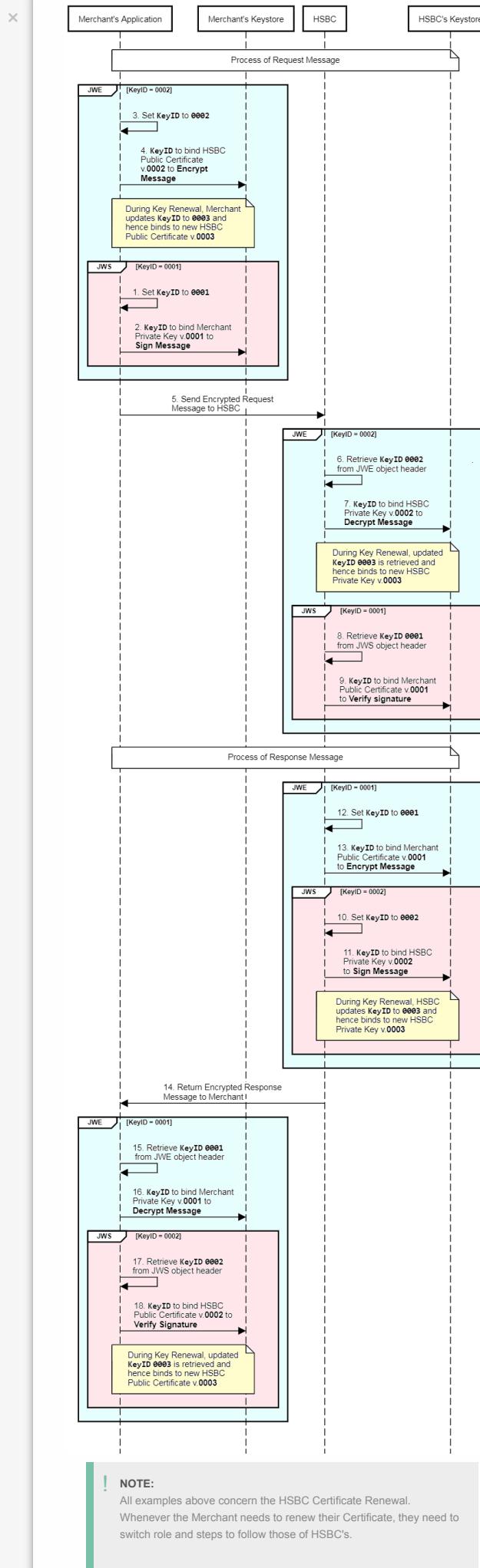
- OrderInput
- OrderOutput
- Order
- PaymentInput
- PaymentPatch
- PaymentOutput
- PaymentWebhook
- Payment
- RefundInput
- RefundOutput
- Refund
- Item
- Card
- HAL
- Exception
- System
- Callback
- Metadata

REFERENCE

- Lifecycle of Cryptographic Keys
- Key Generation & Exchange
- Key Maintenance
- Key Renewal

DISCLAIMER

Disclaimer



Disclaimer

IMPORTANT NOTICE



INTRODUCTION

Description

Update Log

How to Read this Document

Features Overview

GETTING STARTED

How to Connect

API Gateway URL

API Authentication

User Identification

Connection Security

Message Security

Sign & Encrypt

Decrypt & Verify

Summary

How to make API request

with Plain Message

with Data Encryption

Data Type Overview

FAQ

SSL Connection

Message Encryption

JOSE Framework

API OPERATIONS

Orders

Create Order

Retrieve Order by ID

Payments

Create Payment for an Order

Retrieve Payment by ID

Update a Payment

Refunds

Create Refund for a Payment

Retrieve Refund by ID

Webhooks

Payments

API SCHEMA

Schema Definitions

OrderInput

OrderOutput

Order

PaymentInput

PaymentPatch

PaymentOutput

PaymentWebhook

Payment

RefundInput

RefundOutput

Refund

Item

Card

HAL

Exception

System

Callback

Metadata

REFERENCE

Lifecycle of Cryptographic Keys

Key Generation & Exchange

Key Maintenance

Key Renewal

DISCLAIMER

Disclaimer

This document is issued by The Hongkong and Shanghai Banking Corporation Limited, Hong Kong ("HSBC"). HSBC does not warrant that the contents of this document are accurate, sufficient or relevant for the recipient's purposes and HSBC gives no undertaking and is under no obligation to provide the recipient with access to any additional information or to update all or any part of the contents of this document or to correct any inaccuracies in it which may become apparent. Receipt of this document in whole or in part shall not constitute an offer, invitation or inducement to contract. The recipient is solely responsible for making its own independent appraisal of the products, services and other content referred to in this document. This document should be read in its entirety and should not be photocopied, reproduced, distributed or disclosed in whole or in part to any other person without the prior written consent of the relevant HSBC group member. Copyright: HSBC Group 2019. ALL RIGHTS RESERVED.