DBS EXTERNAL API GATEWAY

CUSTOMER ONBOARDING GUIDE

Version 3.4

DBS makes no warranties or representations with respect to the content hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. DBS assumes no responsibility for any errors that may appear in this document. The information contained in this document is subject to change without notice. DBS reserves the right to make any such changes without obligation to notify any person of such revision or changes. DBS makes no commitment to keep the information contained herein up to date.

Table of Contents

Technical Architecture of DBS EXTERNAL API GATEWAY

Figure 1 details the system architecture of DBS EXTERNAL API GATEWAY system. The network connection to DBS will be over the Internet.

Encryption software must be installed at Customer’s Backend Application Server to perform the necessary encryption and signing of files.

Security Features of DBS EXTERNAL API GATEWAY includes:

- Secured communication channel using SSL
- Confidentiality, integrity and authenticity of the message using PGP or JWT encryption
- Digitally signed using PGP or JWT
- Acknowledgement of message received through HTTPS JSON response

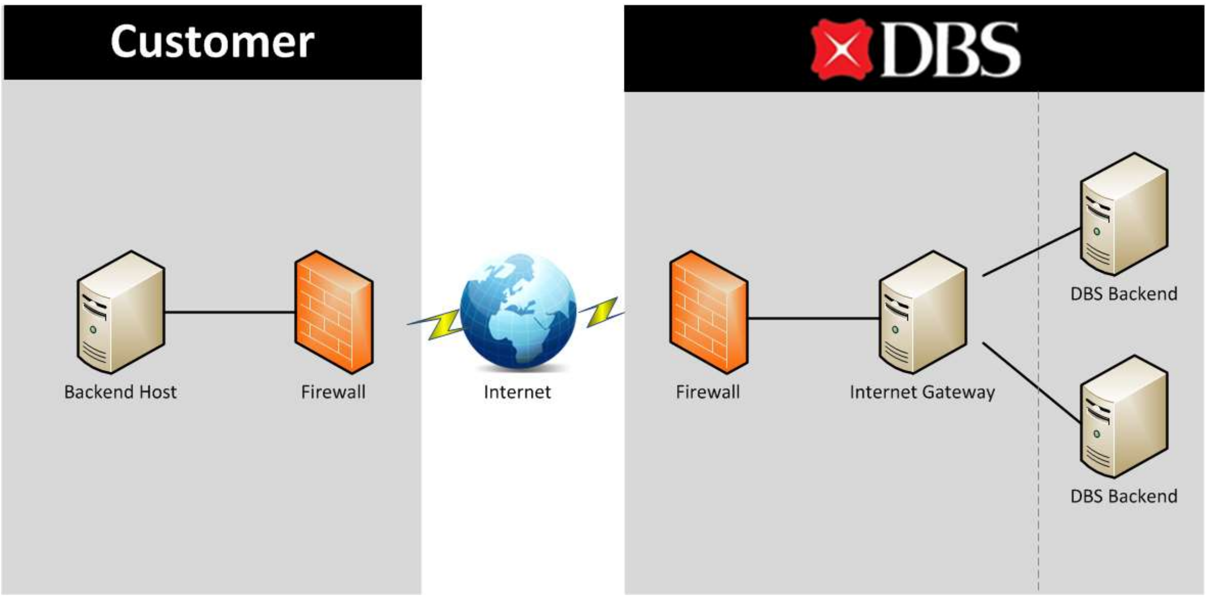

Figure 1 : DBS EXTERNAL API GATEWAY Network Architecture

1 Introduction

This section documents the purpose, background and scope of this DBS EXTERNAL API GATEWAY Onboarding Guide. The target audiences are DBS EXTERNAL API GATEWAY customer's technical team.

1.1 Purpose

This guide provides an overall picture on DBS EXTERNAL API GATEWAY network architecture and specifies the onboarding activities required by customers who would like to subscribe to DBS EXTERNAL API GATEWAY API services.

1.2 Background

The primary business objective of DBS EXTERNAL API GATEWAY is to facilitate customers to be able to connect to DBS services via online APIs. This provides an additional digital channel for customers such as online sites and payment providers, while improving the service quality delivered to DBS EXTERNAL API GATEWAY customers.

1.3 Scope

The guide details the mandatory setup activities and information to be exchanged between DBS and DBS EXTERNAL API GATEWAY customer during the onboarding process. The list of items to be discussed in this guide includes:

1. Technical architecture of DBS EXTERNAL API GATEWAY
2. Message transfer format
3. Encryption and decryption
4. Information to be exchanged between DBS and customers
5. Onboarding activities to be carried out by DBS and customers

1.4 Requirements

This section describes the requirements for onboarding to DBS EXTERNAL API GATEWAY.

Network

- Internet connection to DBS EXTERNAL API GATEWAY
- Firewall rules to permit network traffic between DBS and DBS EXTERNAL API GATEWAY customer

Encryption Software

Pretty Good Privacy (PGP) encryption is used for the encryption/decryption and signing/verification of the message.

Alternatively, JSON Web (JW) Encryption and Signing method can also be used for the encryption/decryption and signing/verification of the message.

Refer to section 1.6 for more information on encryption and decryption, signing and verification.

Each party is responsible to ensure that the preparatory setup (e.g. hardware, software, network, firewall, information exchange etc.) is completed before testing or implementation in production.

1.5 Message Transfer Format

The DBS EXTERNAL API GATEWAY provides a collection of REST APIs that can be called. An API can be called via a HTTPS request. The message format used by DBS EXTERNAL API GATEWAY is in JSON format. JSON is easy to parse and generate, thus DBS adopts the JSON standard and customer shall adopt the same JSON standard which allow overflow/over population of the JSON objects.

A message typically consists of 3 parts – the header, body(payload) and signature.

The header is used to identify the type of message and to route it to the correct API.

The payload is then Encrypted and Digitally signed using PGP mechanism, while if using the JWE (JSON Web Encryption) and JWS (JSON Web Signature) mechanism then payload is digitally signed and then encrypted.

PGP Message	JWT Message	Description
Header	Header	HTTP Headers
Body (Encrypted using receiver's public key)	Body (Signed using sender's private key)	Plain JSON Payload
Signature (Encrypted payload is signed using sender's private key)	Encryption (Encrypt signed payload using receiver's public key)	Digitally Signed and Encrypted JSON Payload

Table 1: Sample message Overview

The sample message will be provided as part of API specification document.

1.6 Message Encryption

The following encryption software are supported by DBS EXTERNAL API GATEWAY:

1. Pretty Good Privacy (PGP)

- Supports minimum of RSA 2048-bit key size and AES encryption.
- Complies with the PKCS#7 standard
- The recommended key pair algorithm will be RSA 2048 bit
- For more information, please refer to www.pgp.com
- PGP keys should be strictly generated from customer's server only and not by any other means.

Symmetric Key Encryption and Signature Algorithm

Customer recommended to comply to below encryption algorithm when encrypting and signing the payload.

1. Payload to be encrypted and then signed in **One Pass** method.
2. Compression Algorithm – **ZIP**
3. Symmetric Key Algorithm – **AES256**
4. Hash Algorithm - **SHA256, SHA384, SHA512**
5. Signing method – **Compressed**

Bank standard Allowed Algorithms

Hash Algorithm – SHA256, SHA384, SHA512

Symmetric Key Algorithm - AES256

Two pairs of private/public PGP keys are involved - one pair for Encrypt/Decrypt and another pair for Sign/Verify.

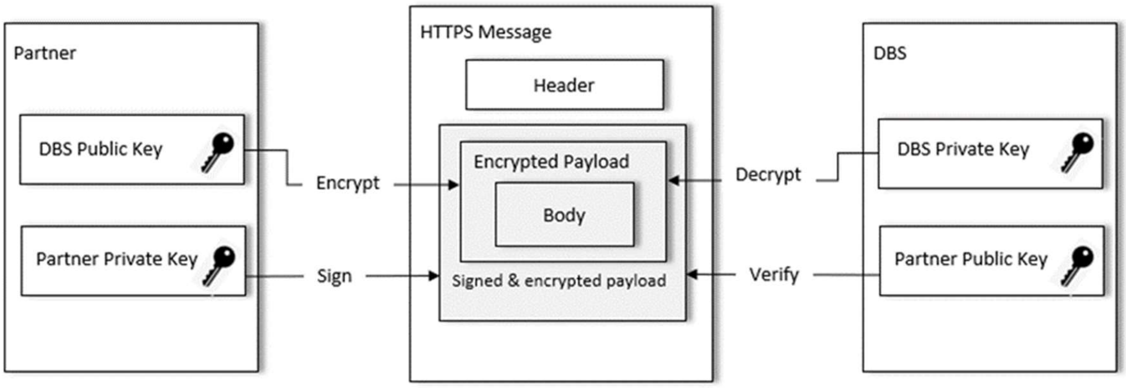

Figure 2: PGP Message Encryption Flow for Inbound API

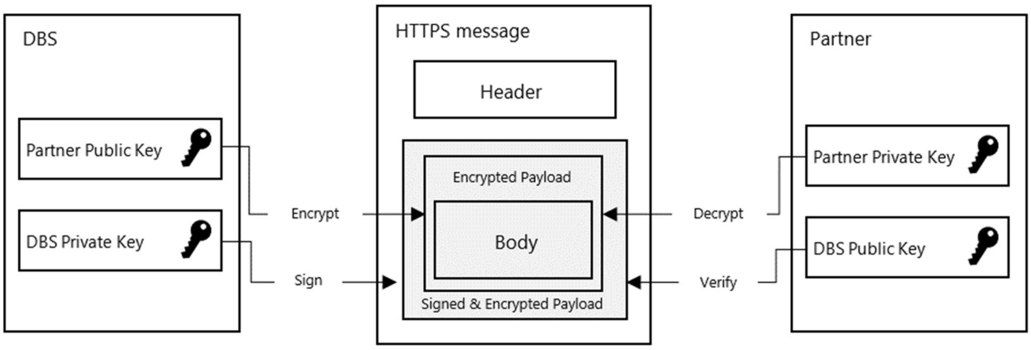

Figure 3: PGP Message Encryption Flow for Outbound APIs (e.g. ICN/IDN)

Generation of PGP key pairs

GNU Privacy Guard (GnuPG) tool can be used for generating and managing the PGP keys. Note that keys should be generated without a passphrase.

http://www.gnupg.org/

Example commands:

- Create a PGP key:

  ```
  gpg --gen-key
  ```

- View the PGP key:

  ```
  gpg -a --export
  ```

- Exports a public key to a file:

  ```
  gpg --export -u 'UserName ' -a -o public.key
  ```

  (or)

  ```
  gpg --armor --export <keyid>
  ```

- Exports a private key to a file:

  ```
  gpg --export-secret-keys -u 'UserName ' -a -o private.key
  ```

  (or)

  ```
  gpg --armor --export-secret-keys <keyid>
  ```

- Lists the private keys:

  ```
  gpg --list-secret-keys
  ```

Encryption / Decryption PGP

Encryption: Public key will be shared with the customer who is encrypting the payload using PGP.

Decryption: DBS will hold the private key for decryption of the payload.

Organization ID (ORG-ID) needs to be specified in the request header. Example: X-DBS-ORG_ID = SGSP02.

Sign / Verify PGP

Sign: Customer will hold the private key and will use it to sign the payload.

Verify: Public key will be shared with DBS for verification of the payload.

After decryption and verification is successful, the decrypted message payload will be sent to the back-end systems in DBS for processing. If there is any failure, an appropriate security related error message will be returned back to the customer.

2. JWT (JSON Web Token)

- JWT Encryption and decryption is done using RSA key pairs
- The payload should be signed then encrypted.
- RSA key length should be at least 2048 bits.
- The RSA public key extension can be .pem format.
- JWT keys should be strictly generated from customer's server only and not by any other means.

Encryption and Signature Algorithm

Customer needs to comply to below encryption algorithm when signing and encrypting the payload.

1. JWS Signature Algorithm - **RS256**
2. Encryption Method Algorithm - **A128CBC-HS256, A256CBC-HS512**
3. JWE Algorithm - **RSA-OAEP-256**

Two pairs of private / public keys () are involved - one pair for Encrypt/Decrypt and another pair for Sign/Verify.

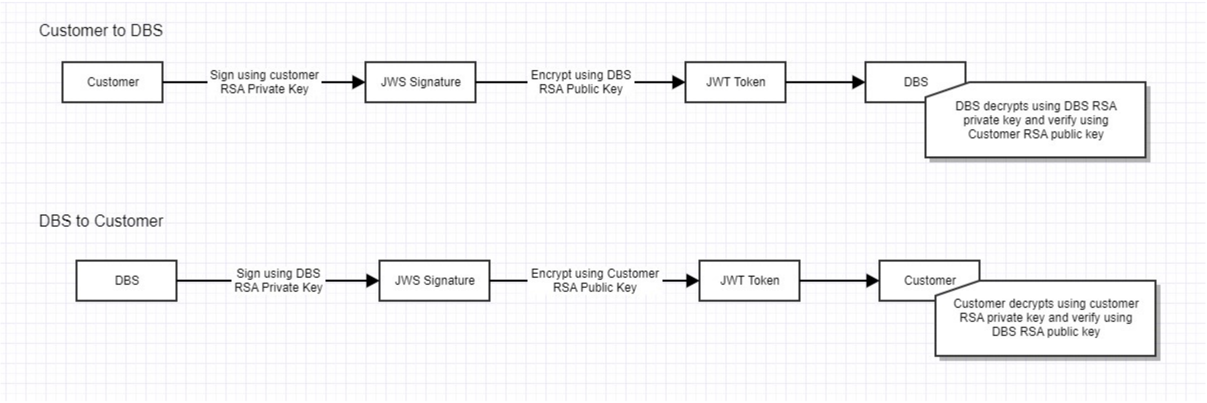
Customer to DBS
Customer
Sign using customer RSA Private Key
JWS Signature
Encrypt using DBS RSA Public Key
JWT Token
DBS
DBS decrypts using DBS RSA private key and verify using Customer RSA public key
DBS to Customer
DBS
Sign using DBS RSA Private Key
JWS Signature
Encrypt using Customer RSA Public Key
JWT Token
Customer
Customer decrypts using customer RSA private key and verify using DBS RSA public key

Figure 4: JWT Message Encryption Flow

Encryption / Decryption JWT

Encryption: RSA Public key will be shared with the customer who is encrypting the payload using JWT.

Decryption: DBS will hold the private key for decryption of the payload.

ORG-ID needs to be specified in the request header. Example: X-DBS-ORG_ID = SGSP02.

Sign / Verify JWT

Sign: Customer will hold the private key and will use it to sign the payload.

Verify: RSA Public key will be shared with DBS for verification of the payload.

After decryption and verification is successful, the decrypted message payload will be sent to the back-end systems in DBS for processing. If there is any failure, an appropriate security related error message will be returned to the customer.

JWT Claims

Payload: Customer/DBS will send the api payload JSON in this claim.

issueTime: Customer/DBS need to send the token issue time in the following format ("yyyy-MM-dd'T'HH:mm:ss.SSSZ")

issuer: Customer need to send the issuer with DBS ORG ID.

Generation of RSA key pairs for JWT

OpenSSL tool can be used for generating RSA keys.

To Create RSA Private Key:

Example commands:

```
openssl genrsa -out private.pem 2048
```

To Create RSA Public Key from RSA Private Key:

Example commands:

```
openssl rsa -in private.pem -outform PEM -pubout -out public.pem
```

1.7 DBS Transport Layer Security standards

- SSL connection TLS 1.2 should be implemented for TLS support others are not supported.

- A Cipher Suite is a suite of cryptographic algorithms used by an SSL connection. Ciphers associate with RSA, AES128, AES256, SHA256 and SHA384 are acceptable.

Standard RFC Cipher Suites that can be used for SSL connection (TLS1.2) – Cloud Layer

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

1.8 Data Retention

All messages transferred through DBS EXTERNAL API GATEWAY will be kept online by backend systems for 90 days before they are archived to offline tapes. All the financial data will be kept up to 7 years on tape based on regulatory requirements.

1.9 Email and SMS Notification

DBS provides an email and SMS notification service to notify customers on the success of certain high value transactions, such as payments.

Depending on the use case, the notification can either be sent to the customer or the customer's customers. For example, in the case of payments initiation, a notification can be send to the initiator (customer's customers) upon a successful transfer of funds.

2 Information Exchange

Before the customer can perform testing with DBS, certain information and keys will need to be exchanged with DBS.

The following items need to be exchanged between the customer and DBS.

Environment	**Production**	**UAT**	**Simulated Test Environment**
Incoming to DBS			
Source Public IP	<Customer to provide>	<Customer to provide>	<Customer to provide>
Destination Public IP	**Cloud Env Details** enterprise-api.dbs.com	**Cloud Env Details** uatcld-enterprise-api.dbs.com	**Cloud Env Details** testcld-enterprise-api.dbs.com
Destination Port	443	443	443
CA Signed SSL cert	<DBS to provide>	<DBS to provide>	<DBS to provide>
Outgoing from DBS			
Source Public IP	**Cloud Env Details** 3.0.208.98 13.228.212.230 13.251.55.228 103.4.36.27 103.4.38.27 115.42.149.8 203.116.209.20 210.79.56.27 210.79.58.27	**Cloud Env Details** 18.139.156.226 3.1.152.142 52.77.152.255 203.125.122.65 45.65.2.156	**Cloud Env Details** 18.139.156.226 3.1.152.142 52.77.152.255 203.125.122.65 45.65.2.156
Customer URL	<Customer to provide>	<Customer to provide>	<Customer to provide>
Customer Port	443	443	443
CA Signed SSL cert	<Customer to provide>	<Customer to provide>	<Customer to provide>
PGP/JWT Key Exchange			
Encryption Public Key	<DBS to provide>	<DBS to provide>	<DBS to provide>
Signature Verification Public Key	<Customer to provide>	<Customer to provide>	<Customer to provide>

Table 2: Information Exchange

3 On-Boarding Activities

The following subsection documents the activities and testing required at DBS and customer.

3.1 List of Activities

Before the interface testing could be performed, the following activities will need to be carried out:

No	Activity Item	Action Party	Duration	Remarks
1	Onboarding of profile			Items required (Simulated Test Environment, UAT & Production): ▪ API subscriptions ▪ Profile entitlements
2	Network Information Exchange	DBS & Customer	1 day	Items required (Simulated Test Environment, UAT & Production): ▪ IP Addresses ▪ Port number
3	Raise firewall change request for UAT & Production	DBS & Customer (where applicable)	1 day	3 working days lead time to raise necessary change request for firewall rules change
4	Key Exchange	DBS & Customer	3 days	Items required (Simulated Test Environment, UAT & Production): ▪ PGP public and private keys
5	UAT Environment Setup	DBS	5 days	
6	Connectivity Test on UAT	DBS & Customer	2 days	Message transmission for both request and return. Encryption / decryption and sign / verify must work for both parties.
7	UAT transaction testing	Customer	5 days	API testing
8	UAT sign-off	Customer	1 day	
9	Raise change request for production deployment	DBS & Customer (where applicable)	1 day	2 weeks lead time to raise necessary change request for production deployment
10	Production deployment	DBS & Customer (where applicable)	1 day	
11	Connectivity test on Production	DBS & Customer	1 day	Message transmission for both request and return. Encryption / decryption and sign / verify must work for both parties.
12	Live Verification on Production	DBS & Customer	1 day	Customer to send a live transaction message. DBS to monitor end-to-end.
13	Post Implementation	DBS & Customer	3 days	Review of the entire implementation for feedback.

Table 3: List of activities for DBS and customer for Onboarding

Note: Estimated man-days may vary depending of the scope and complexity of the file transfer requirements and customer's environment.

3.2 Testing Requirements

In order to onboard to DBS EXTERNAL API GATEWAY, customers would need to perform testing with DBS before implementing in production. The testing includes both Connectivity Testing and User Acceptance Testing.

3.2.1 Connectivity Testing

The objective of Connectivity Testing includes the following:

- Telnet
- PGP Encryption / Decryption
- PGP Sign / Verify
- Message transmission

3.2.2 Simulated Testing

The objective of Simulated Testing includes the following:

- Simulated Test environment to do preliminary API testing using Mock data.
- Message format
- Response message – message format & rejection codes

3.2.3 User Acceptance Testing (UAT)

The objective of UAT includes the following:

- Routing of the message based on the header to the relevant API
- Message format
- Response message – message format & rejection codes

Testing scope varies based on the API that the customer intends to subscribe to.

4 Appendix A: Additional API Specific Requirements

This section describes the additional information required by specific API.

4.1 Retail Customer

No	Client Onboarding Parameters	Values
1	client_id	DBS ORG-ID at DBS EXTERNAL API GATEWAY which would be assigned to corporate customer at the entity level
2	client_secret	<DBS to provide>
3	redirect_uri	<Customer to provide>
4	scope	ddaSetup, retrieveAccounts
5	Auth Code Expiration	3 mins
6	Access Token Expiration	15 mins

Table 4: List of activities for OAuth Onboarding for Retail Customers

4.2 Ideal Customer (ERP Integration)

No	Client Onboarding Parameters	Values
1	client_id	DBS ORG-ID at DBS EXTERNAL API GATEWAY which would be assigned to corporate customer at the entity level
2	client_secret	<DBS to provide>
3	redirect_uri	<Customer to provide>
4	Auth Code Expiration	30 seconds
5	Refresh Token Expiration	90 days
6	Access Token Expiration	4 hours
7	Cancel / Error Screen / Back button URL	<Customer to provide>
8	Learn More URL	<Customer to provide>
9	Contact Us URL	<Customer to provide>
10	Logo	<Customer to provide>

Table 5: List of activities for OAuth Onboarding for Ideal Customers

Below are some exceptional scenarios to be taken care of with action required from partner side:

Scenario	Expected Outcome	Error Codes	Action by Partner
Locked IDEAL Account	User can get statements after account is unlocked.	Allow token refresh so that user can resume when account is unlocked	No Action
Deleted IDEAL account	User is unable to get statements.	Error code is A018	Remove token/access upon receiving this error code
Late generation of statement	User can get statements	Error code is MT940003	Perform retry upon receiving this error code
User un-provision statement on IDEAL	User should be informed to perform provision as he\she un-provisioned in Ideal.	Error code is A017	Partner to inform customers to provision upon receiving this error code
SGD accounts not available on Monday	User is unable to get statements.	Error code is IG940003	No Action
ORG-ID passed is incorrect or ORG-ID in http header does not match payload ORG-ID	Unable to do transaction	A001	Verify and pass correct ORG-ID
Maximum transaction transmission is exceeded	User can do transaction successfully	A002	Perform retry upon receiving this error code
Invalid Request	Unable to do transaction	A003	Verify the JSON format of payload and resend
Key pair used for encryption and signing are incorrect	Unable to decrypt and verify request	A004	Verify keys and mechanism & algorithms for encrypt and sign service. Refer section 1.6 for more info.
DBS External API Gateway not able to connect to backend.	User can do transaction successfully	A005	Perform retry after some time upon receiving this error code, if received again contact DBS support.

Table 6: Exception Scenarios

4.3 Synchronous and Asynchronous APIs Exceptional Handling

Below are **synchronous** API and **asynchronous** API exceptional handling diagram:

i) Synchronous API

Customer can retry up to 2 times with the same customer transaction reference but different message id if getting timeout for synchronous API request to fetch the latest transaction status.

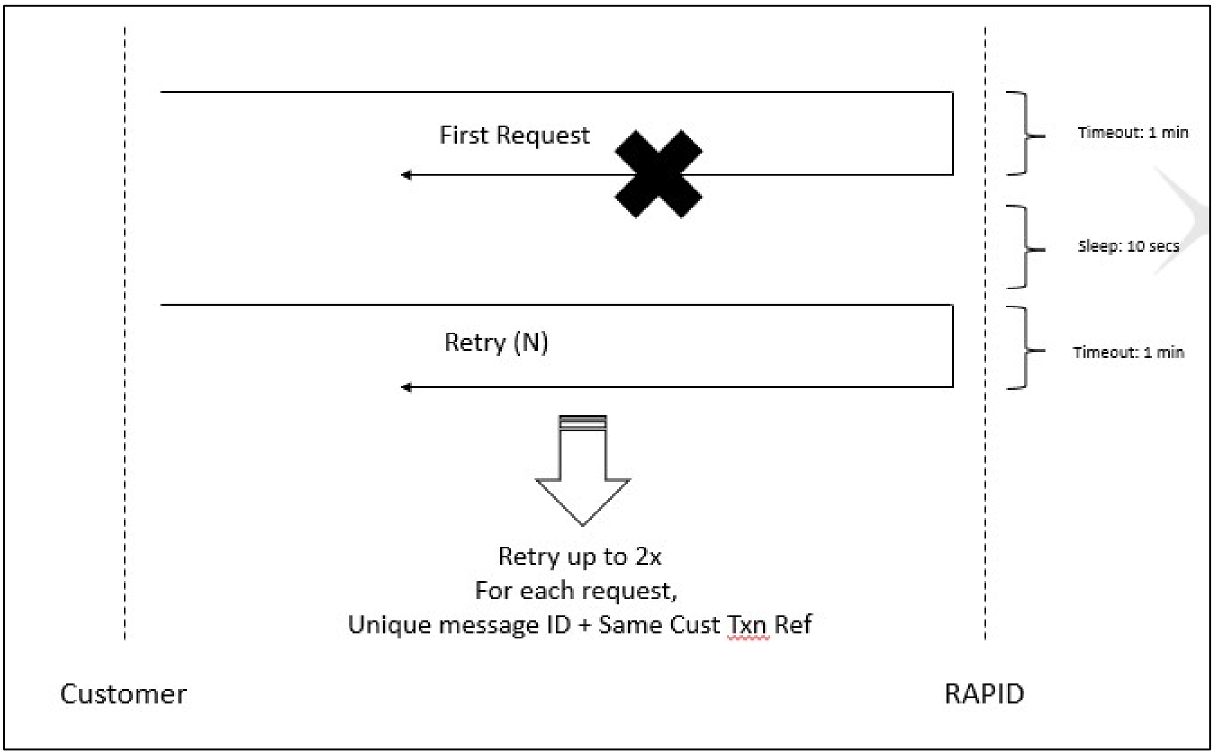

Figure 5: Synchronous API Exceptional Flow

ii) Asynchronous API - DBS Retries (applicable for ICN only)

In the event that the bank did not receive a http 200 response for the ICN API message that it sent to customer's server (i.e. timeout encountered),, the bank will retry once and fire the same ICN API message to customer's server again. Customers should implement a retry handling logic to detect same bank transaction reference and / or message ID in ICN API messages received and ignore the subsequent ICN API message as applicable.

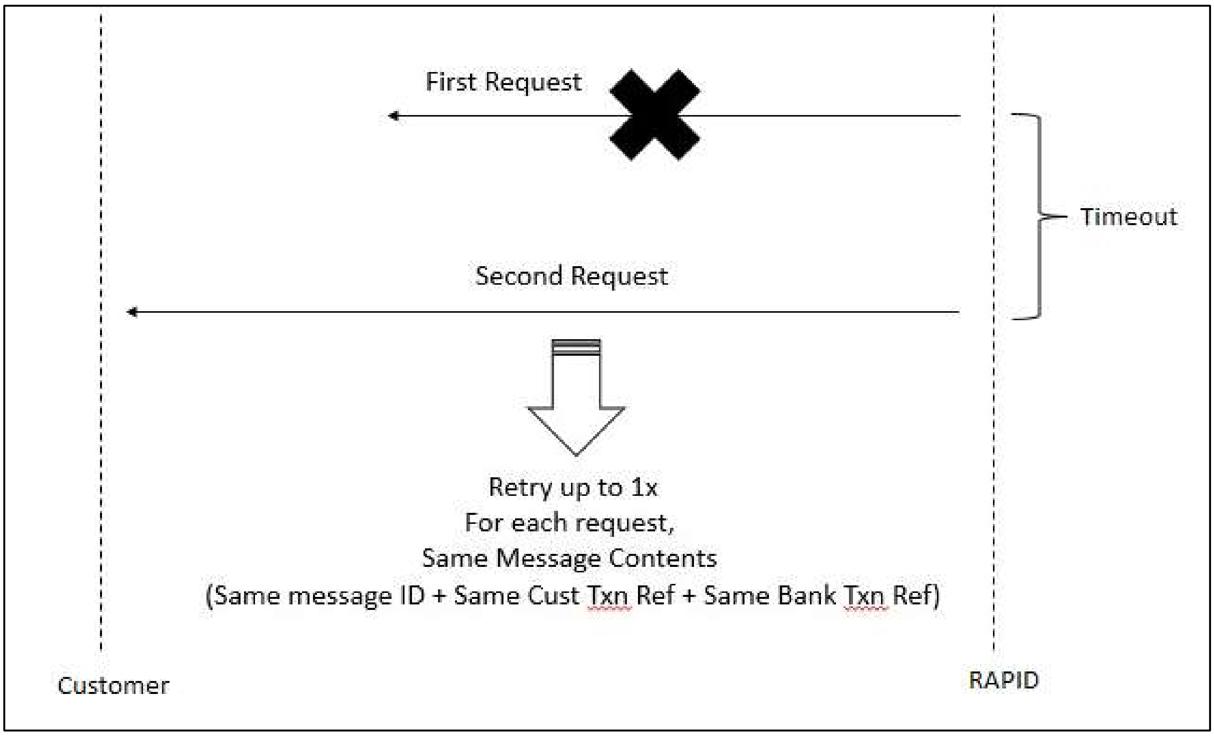

Figure 6: Asynchronous API Exceptional Flow - DBS Retries (applicable for ICN only)

iii) Asynchronous API - Consumer Scan / Pay Multiple Times (applicable for ICN only)

When consumers scan and pay the same QR more than one-time, corporate customers may also receive duplicate ICNs. These ICNs would contain the same customer transaction reference but have different bank transaction reference. The different bank transaction references represent the multiple credits that have occurred on the corporate customer's account (i.e. consumers pay more than once to the corporate customer's account).
In the event that the bank did not receive a http 200 response for the ICN API message that it sent to customer's server (i.e. timeout encountered), the bank will retry once and fire the same ICN API message to customer's server again.

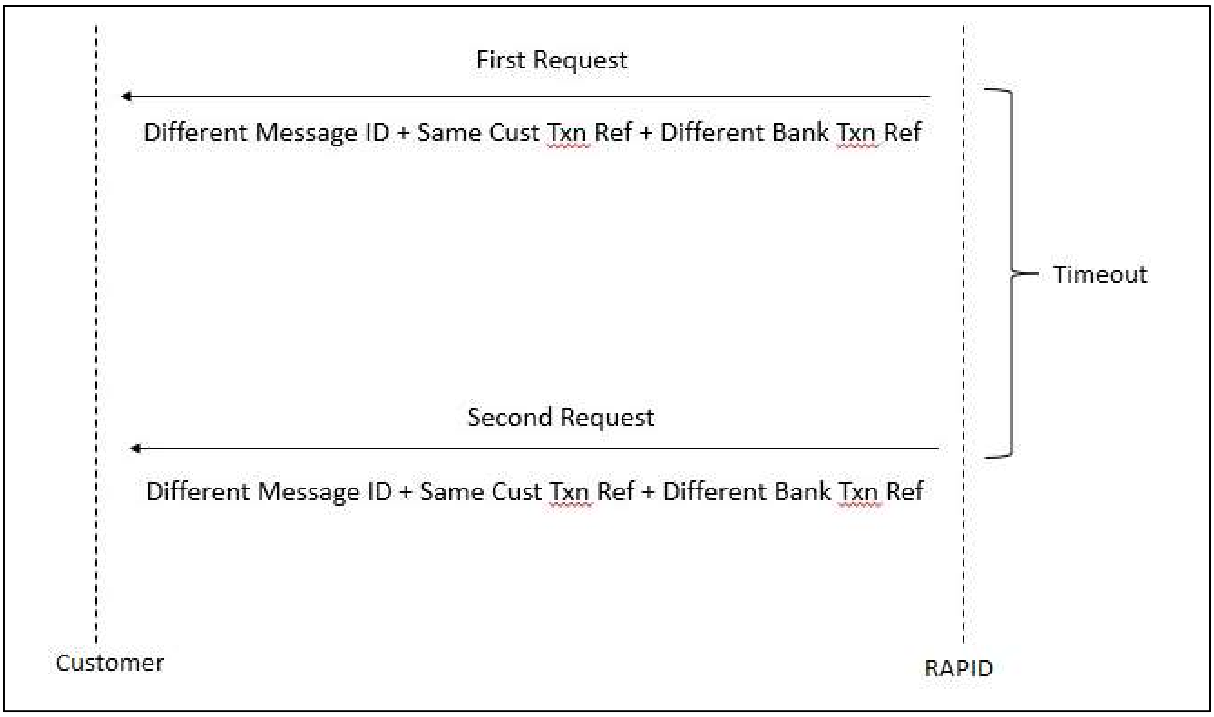
First Request
Different Message ID + Same Cust Txn Ref + Different Bank Txn Ref
Timeout
Second Request
Different Message ID + Same Cust Txn Ref + Different Bank Txn Ref
Customer
RAPID

Figure 7: Asynchronous API Exceptional Flow - Consumer Scan / Pay Multiple Times (applicable for ICN only)

4.4 Downtime Notification Message

DBS has scheduled maintenance from time to time and you will be notified via emails in advance with the date, start and end time.

Where required, please help to notify your customers of the scheduled maintenance, or place a notification message on your platform.

4.5 Trade APIs

Trade customers would be assigned a unique ORG-ID with account number for RAPID API subscriptions. Each ORG-ID is unique and must correspond to a legal entity registered with the local regulatory body.

For all trade documents (supporting) sent by customer to the bank, the customer should follow the following file naming convention.

DocumentName: File Naming Convention

<orgID><tradeProductType><documentName><DDMMYYHHMMSS> ▪ <doctypeExtension>

Where

- *orgID = the unique identifier assigned by DBS to a legal corporate entity*
- *tradeProductType =*
    - EDC
    - APF
    - ARF
    - LC
    - IBLC
- *documentName must be perpetually unique,*
- *DDMMYYHHMMSS must be the date / time the document was uploaded to DBS, and the*
- *doctypeExtension must reflect the actual document type of the attachment.*
- *Documents must not be more than 5mb in size.*

5 Appendix B: Frequently Asked Questions

This section describes the FAQ in different categories.

5.1 Technical Parameter

5.1.1 Does DBS accept dynamic IP address for whitelisting?

No, DBS will accept only static IPs for whitelisting.

5.1.2 Does DBS accept a range of IPs for whitelisting?

Yes, DBS will accept the IP range as long as they are static and IPv4. Preferable accepted range is from /24 to /32 and need to provide justification for wider range of IPs.

5.1.3 Can we provide IP address instead of domain name server (DNS) for DBS outbound APIs?

No, it is mandatory to provide DNS for proxy whitelisting for all DBS outbound APIs (e.g. ACK2/ACK3 for TT, ACT, IDN, ICN, etc).

5.1.4 Why should I submit SSL certs to DBS for incoming notifications?

Your SSL certs are used for below 2 purposes

1) For SSL validation: While DBS connects to you, firstly, we will validate your SSL certs for the certificate name (“Issued To”) against the URL which you have shared with us and secondly, the certificate presented during handshake by your server to DBS will be validated against the Trusted CA in our DBS certificate store as security feature.
2) For Expiry Notification: If the SSL cert had expired meaning they are no longer in Trusted CA and thus DBS will not post any ACKs/notification messages to you. To cater this, whenever the SSL certs nearing its expiration, DBS will approach you to share the latest certs.

5.1.5 Does DBS accept self-signed/wildcard SSL certs?

DBS will accept self-signed/wildcard SSL certs for testing purposes only. For production, DBS will only accept valid CA certs from a trusted authority.

5.1.6 How to import SSL certs?

You may look into our sample codes on how to import SSL certs.

5.1.7 Can DBS add a new header parameter for Intraday Credit Notification (IDN)/Incoming Notification (ICN) API as requested by customer?

Yes, but the header value must be static. DBS will not accept dynamic values in the header section

5.1.8 Does DBS accept OAuth 2.0 with dynamic redirect URL?

No, only static redirect URLs are accepted as DBS will have to configure the redirect URL as a system parameter for authorization purposes.

5.1.9 Does DBS accept OAuth 2.0 with multiple redirect URLs?

Yes, DBS will allow multiple redirect URLs to be configured in our system.

5.1.10 Does DBS accept OAuth 2.0 with query string character in redirect URL?

Yes, DBS will accept "?" query string character in the redirect URL.

5.1.11 Apart from auth code, will there be any other information (like session ID) passed via redirect URL?

No, DBS will pass only the auth code and no other information as it doesn't store and the DBS pre login page is itself redirected from customer's website/application

5.1.12 Does DBS support iFrame to integrate the customer’s application with digibank login?

No, DBS does not support iFrame concept to integrate with digibank login

5.2 Encryption & Decryption

5.2.1 How to generate PGP keys?

If you are having trouble generating valid PGP keys, we can share a proprietary PGP generation tool to help you generate keys in a simpler, more intuitive way. Please request the implementation manager to share this tool if required.

5.2.2 How to ensure the PGP algorithm is accepted by the bank?

Please ensure that:

1) PGP Key is valid (2048 bits)

2) Hash algorithm: SHA256

3) Encryption algorithm: AES256

4) Compression: zip

5.2.3 How to encrypt/sign or decrypt/verify in one pass method?

The one-pass method means that you encrypt and sign at once, rather than encrypt then sign the encrypted message after. This allows the receiving party (DBS) to also decrypt and verify together in one go. When testing, please set up the according header and encrypt only the payload. You can follow our sample code directly and set encrypt.setSigning(true) so that signing happens by default after encryption. For more details and walkthrough, please request for the specific sample code for the programming language you are using (e.g. C#, Java).

5.2.4 Do we need to encrypt the HTTP Header part as well?

No, DBS will first validate the HTTP header to ensure the API call is from authorised sender. Only the JSON payload needs to be encrypted and signed with PGP/JWT key as it may contain sensitive financial data.

5.3 Connectivity & UAT Testing

5.3.1 How long does it take to whitelist the IP addresses at DBS?

IP addresses whitelisting will take 3 to 5 working days at DBS.

5.3.2 Why did the incoming connectivity check to DBS server fail?

Please ensure that:

1) The IP address that you are making the connection from is the same as the one provided in the Technical Parameters for DBS to whitelist

2) You are calling the URL for the correct environment:

Environment	URL
Staging	https://testcld-enterprise-api.dbs.com/api/rg/healthcheck/v4/enquiry/status
UAT	https://uatcld-enterprise-api.dbs.com/api/rg/healthcheck/v4/enquiry/status
PROD	https://enterprise-api.dbs.com/api/rg/healthcheck/v4/enquiry/status

5.3.3 How do I test QR codes with ICN ?

You may send the QR code to DBS. We will scan the QR, mock up the ICN response with the payment details and send the ICN message to you.

5.3.4 How do I test IDN and ICN?

You can provide us with the payment details (e.g. Transaction type, Proxy type). We will mock up the IDN/ICN response with details and send the message to your specified IDN/ICN URL.

5.3.5 How can I test balance enquiry (ABE) & Account Range Enquiry (ARE)?

The test environment has readily available mocked up data for ARE and ABE. You do not need to send transactions first in order to call enquiry API.

5.3.6 Can I make test payments (eg. ACT, TT, etc) and check for these transactions with ARE?

Our test environment only contains mock data and does not store test transactions made by customers. However, you can test this feature during Live validation in Production.

5.3.7 I have tested FX Booking API. How should I go about with settlement testing?

You will need to trigger an ACT/TT request for currency exchange/remittance. In the request message, you will need to include the FX contract number, buying and selling currencies.

5.3.8 How many retries for ICN if DBS doesn’t receive HTTP 200 OK response from you?

DBS will resend ICN only one time and will not resend again if it’s unsuccessful. In such cases, DBS Ideal Rapid support team will contact you directly to inform about this.

5.3.9 Will there be a retry for Ack 2/3 if there is any downtime at our side?

No. DBS will not resend ACKs. In such cases, DBS Ideal Rapid support team will contact you directly to inform about this.

5.4 Functional

5.4.1 Use cases on different type of payments like ACT, RTGS, TT, FAST, FPS, etc. On what scenario to use which payment?

Markets	Payment Type	Use Case	Currency	Intra-bank/ Interbank	FX/Non-FX	Cut-off/24x7
All	ACT	Local Intra-bank payments (DBS to DBS)	Vary for different markets	Intra-bank	Both	1. 24x7: All markets non-FX payment except CN 2. Cut-off: All markets FX payment
	TT	Overseas payment	Vary for different markets	Both	Both	Cut-off
		Local interbank FX payment		Interbank	FX	
CN	CUP	Real-time local payments	CNY	Both	Non-FX	24x7
	CNAPS	Local interbank high value payments		Interbank		Cut-off
HK	FPS	Real-time local payments	HKD, CNY	Both	Non-FX	24x7
	CHATS	Local interbank high value payments	HKD, CNY, USD	Interbank		Cut-off
ID	RTOL	Real-time local payments	IDR	Both	Non-FX	24x7
	RTGS	Local interbank high value payments		Interbank		Cut-off
IN	UPI	Real-time local payments	INR	Both	Non-FX	24x7

	RTGS	Local interbank high value payments		Interbank		Cut-off
SG	FAST	Real-time local payments	SGD	Both	Non-FX	24x7
	MEPS	Local interbank high value payments		Interbank		Cut-off
TW	eACH	Real-time local payments	TWD	Both	Non-FX	24x7
	FISC	Local interbank high value payments		Interbank		Cut-off

5.4.2 Can you send another real-time transaction with the same customer reference if DBS does not respond with either a 'ACTC/RJCT' transaction status? Would there ever be a scenario where there are duplicate real-time transactions for the same transaction reference number?

Each Message ID and customer reference has to be unique. We expect customers to practice good session management to keep track of and manage all user sessions they have with their systems. Good session management is an important hygiene factor to ensure customers are able to scale up and handle high concurrency throughputs, protect their data integrity (e.g.avoid duplicates/ incorrect statuses) and ensure no operational impact (e.g. rework due to duplicates).

If you resend a transaction with the same customer reference upon no response timeout, DBS will respond with a duplicate and indicate the latest status of that transaction. Otherwise, if duplicate is not found, DBS will process the new transaction and respond with the corresponding transaction status.

Note: If you send multiple transactions with the same customer reference simultaneously at the same time to the bank, there is a risk of duplicates due to the concurrent channel processing design. It is therefore important that you only resend the transaction with the same customer reference upon timeout.

5.4.3 How do I get the actual transaction status for real-time payments if it is not returned in the response message?

You can send another API request with different message ID but same customer reference to enquire the transaction status after 30 seconds of the original transaction sent.

5.4.4 Given that the receivingParty name can only be 35 chinese characters, what can I do if it exceeds the limit?

You may utilize the beneficiary address field for the remaining part of receivingParty name.

5.4.5 What is the purpose of debitAccountAmount?

The DebitAccountAmount will be relevant if there is fxContractRef. For transactions without fxContractRef, txnAmount will take precedence over debitAccountAmount.

For Example:

- txnAMount (Mandatory parameter Input): 100
- txnCcy (Mandatory parameter Input): USD
- debitAccountCcy (Optional parameter Input): SGD

Result: 100 USD will be paid out, with the SGD equivalent (of 100 USD) debited, based on DBS prevailing board rates.

5.4.6 What is the difference between ACK1/ACK2/ACK3 for payment transactions?

ACK1 is to inform you that DBS has received the API request and completed schema validation for the JSON payload.

ACK2 is to inform you that DBS has completed the business validation of the API request and transaction is being process by the back office for accepted transaction.

ACK3 is to inform you that DBS has processed the transaction and typically received within ~15 min after the transaction is processed, though this may vary depending on the type of API and back office validation. The final transaction status will be updated after transaction is being processed by beneficiary bank, so you can reach out to DBS BizCare Team to enquire the final transaction status.

5.4.7 What is the different between ACK1/ACK2 for HK eDDA Setup?

ACK1 is to inform you that DBS has received the API request and completed schema validation for the JSON payload.

ACK2 is to inform you of the final status for eDDA setup.

5.4.8 Can we perform ABE by inputting virtual account no. instead of master account no. in the request message?

No, because virtual accounts are regarded as a channel for crediting fund to the master account. You must input the master account number in the request message to trigger balance enquiry.

5.4.9 Will there be any funds kept in the virtual account (VA)?

No, the funds will go directly into the master account that is linked to the virtual account. Virtual account serves only as a mirror account for the actual master account.

5.4.10 How many transactions does ARE support? What if the number of transactions that I wish to check exceed 1000?

ARE enquiries are limited by 1000 transactions in a single call. However, you may check Credit and Debit transactions separately.

5.4.11 Will DBS support Joint-All account for SG DDA setup?

No, DBS will only support Joint-Alt account for DDA setup.

5.4.12 Can DBS filter non-SGD multi-currency accounts for SG DDA?

No, you will need to incorporate filter for SGD wallet of a multi-currency account in your design and build.

5.4.13 I made an API call to DBS. Why is the return message a clear JSON payload?

DBS will return a clear JSON payload when the API request is rejected by the gateway because the data in the JSON payload is not sensitive (e.g. Invalid Org ID or Key ID)

5.4.14 Why is my transaction rejected?

<u>For "A" & "I" series error code:</u>

DBS' Gateway or Channel backend has rejected the transaction, you may refer to API specifications or reach out to the Ideal Rapid Support Team to get more info on the rejection.

<u>For other error code:</u>

DBS' back office or beneficiary bank has rejected the transaction, you can refer to API specifications or reach out to the BizCare Team to get more info on the rejection.

5.4.15 Will DBS reject transactions sent after cut-off time?

No, transactions sent after cut-off time will roll-over to the next business day and transaction status will return as "ACWC".

5.4.16 Does DBS accept overflow/overpopulation/underflow in the JSON payload?

Yes, DBS allows overflow/overpopulation/underflow in the JSON payload. Missing mandatory field will cause rejection but missing optional field is acceptable. You should also allow overflow/overpopulation/underflow in the JSON payload returned from DBS.

5.5 Technical Implementation

5.5.1 Are there specific dates for deployment in production?

Yes, DBS has specific green zone dates for customer onboarding in production environment. You may discuss with your implementation manager on setting a target tech live date.

5.5.2 How do I get the PROD profile setup status?

You may check with implementation manager, profile setup should be completed before the target tech live date.

5.5.3 What is live verification (LV) testing?

Live verification testing involves an end to end testing in production environment to ensure that successful connectivity is established between the customer and DBS.

5.5.4 Can I skip live verification testing after production deployment is successful?

No, upon successful deployment in production, a member of your team has to perform a live verification test. This will allow us to address and troubleshoot any potential issues you may face immediately.

6 Appendix C: DBS Support & Contact Details

This section describes the type of support & contact details for different queries.

6.1 Implementation Technical Support

Please send specific enquiry to the DBSRapid Team for technical related queries during implementation.

- Testing Environment related queries. (eg. connectivity, encryption, decryption, etc)
- Sample codes
- UAT Testing related issues/clarification.

Markets	Emails	Hotline	Operating hours (SGT)	
All	dbsrapid@dbs.com	NA	Mon to Fri	9am to 7.30pm

6.2 Post-Implementation Support (Technical)

Please send specific enquiry to the IdealRapidSupt Team for technical related queries at PROD.

- Missing IDN/ICN *(please provide transaction reference)*
- Missing ACK1/ACK2 *(please provide transaction reference/ message ID)*
- Rejection details for transaction rejected by DBS' Gateway or Channel backend ("A" & "I" series error codes)

Markets	Emails	Hotline	Operating hours
All	idealrapidsupt@dbs.com	Primary: +65 8168 5746 Secondary: +65 9185 3079	24x7

6.3 Post-Implementation Support (Business & Operational)

Please send specific enquiry to the DBS BizCare Team for non-technical related queries at PROD.

- Fee & charges
- Product cut-off time
- Account balance queries
- Missing ACK3 & transaction status
- Rejection details for transaction rejected by DBS back office or beneficiary bank
- System downtime

Markets	Emails	Hotline	Operating hours (Local Time)	
CN	BusinessCareCN@dbs.com	400 821 8881	Mon to Fri	9am to 6pm
HK	BusinessCare-HK@dbs.com	(852) 2290 8068	Mon to Fri	9am to 6pm
			Sat	9am to 1pm
ID	BusinessCareID@dbs.com	1500-327	Mon to Fri	8am to 5pm
IN	BusinessCareIN@dbs.com	1800 419 9500 1800 103 6500 +91 44 6632 8000 (oseas)	Mon to Fri & RBI working Saturdays	10am to 5pm
SG	BusinessCareSG@dbs.com	1800 222 2200 +65 6222 2200 (oseas)	Mon to Fri	8.30am to 8.30pm
TW	BusinessCareTW@dbs.com	(886) 2 6606 0302	Mon to Fri	8.30am to 6.30pm