

# Certification Guidelines and UI Best Practices v 1.1

version 1.0.0



## **COPYRIGHT**

The copyright in this work is vested in Specialized Technical Services, and the document is issued in confidence for the purpose only for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under an agreement or with the consent in writing of Specialized Technical Services, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document, or any part thereof, arising directly or indirectly thereafter will be given orally or in writing or communicated in any manner whatsoever to any third party, whether an individual, firm or company, or any employee thereof, without the prior consent in writing of Specialized Technical Services.

This material is submitted with limited rights under the STS disclosure agreement. © Copyright STS (2016)

## Document Overview

**This document covers the guidelines that the entity/merchant will follow to conclude the certification successfully with the STS PayOne smart route/PG so that the entity/merchant will be ready to be moved to production.**

## Smart Route/Payment gateway functions

PG Admin will certify the entity/merchant on the agreed and implemented functions (The merchant may implement all or some of the functions available based on the business needs).

The following are the smart route/payment gateway functions :

- 1- Redirect Pay web
- 2- B2B pay web
- 3- Direct post
- 4- Refund
- 5- Inquiry
- 6- Pre-auth (to be enabled)
- 7- Completion (to be enabled)

All functions should be developed according to the integration guide with the help of the provided examples/sample codes in the integration guide.

## General web site requirements (Merchant Site):

- 1- The organization web site should be accessible using a name service like (*www.domain.ae*)
- 2- The integrated pages should be SSL enabled (HTTPS) with minimum 128 bit real certificate. (*https://www.domain.ae/..* )
- 3- Direct access to the integrated pages should be blocked, even it is recommended to implement the same restrictions for user's privileged pages to force the user to go through the proper application workflow and redirect him to the login page (same rule applies even if there is no user profile management).
- 4- Organization web site user interface supported languages should be communicated to the PG Admin, and all pages should be consistent with the user selected language along all the payment cycle.

**Note:** PG supports Arabic and English interfaces and this can be controlled by the parameters passed by the organization web site to the PG through the redirection. Please refer to the integration guide Pay function for more details.

## Transaction response/status handling :

When the transaction response is received by the merchant, the transaction results should be displayed for the user on the merchant response page in both cases (successful & failed).

The merchant should display the following :

- 1- Transaction ID
- 2- Transaction amount
- 3- Transaction status
- 4- Transaction date & time.

## Broken Transaction Handling :

**Definition : The broken transaction is a payment request that has been submitted from the merchant website towards the smart route/payment gateway but due to some reason the transaction response (Transaction status) has not been received by the merchant website.**

The broken transactions scenario may happen due to many scenarios and the following are examples of the reasons that may cause this business case:

- 1- User reached the smart route/payment gateway and the connection was reset.
- 2- User reached the smart route/payment gateway and the browser closed.
- 3- User reached the smart route/payment gateway and the computer/device switched off.

Having the broken transaction happened, the merchant should make sure that proper handling is implemented to avoid financial impact caused by this case.

The proper handling is to implement the required functionality that will not allow duplicate payment for the same service/product/application from the merchant website until the broken transaction is verified and based on the status the merchant either provides the service/product/application (if the transaction status was received as successful) or request the user to pay again (if the transaction status was received as Failed).

The above described scenario is implemented by checking the transaction status in the merchant side, if no result is found then the application should be blocked and the “inquiry function” should be executed after 20 minutes of the transaction original time.

If the transaction was initiated at 03:00 PM and the merchant system noticed that no result is available for it at the DB level then the user should not be allowed to execute a new transaction till 03:21 PM. At this time the “inquiry function” is invoked and based on the response received for that particular transaction the above business logic is followed.